

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-252607
(P2002-252607A)

(43) 公開日 平成14年9月6日(2002.9.6)

(51) Int.Cl. ⁷	識別記号	F I	テ-マコ-ト*(参考)
H 0 4 L 9/08		G 0 6 F 15/00	3 3 0 Z 5 B 0 8 5
G 0 6 F 15/00	3 3 0	H 0 4 L 12/22	5 J 1 0 4
H 0 4 L 12/22		12/56	2 6 0 A 5 K 0 3 0
12/56	2 6 0	9/00	6 0 1 B

審査請求 未請求 請求項の数49 O L (全 27 頁)

(21) 出願番号 特願2001-31338(P2001-31338)
(22) 出願日 平成13年2月7日(2001.2.7)
(31) 優先権主張番号 特願2000-390926(P2000-390926)
(32) 優先日 平成12年12月22日(2000.12.22)
(33) 優先権主張国 日本(J P)

(71) 出願人 000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号
(72) 発明者 庵 祥子
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内
(72) 発明者 三宅 延久
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内
(74) 代理人 100083552
弁理士 秋田 収喜

最終頁に続く

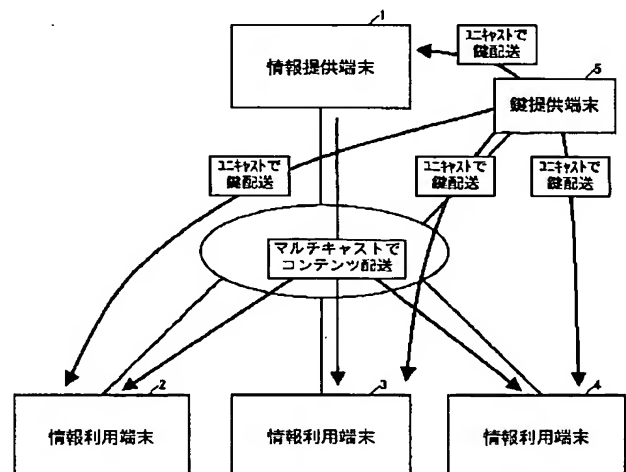
(54) 【発明の名称】 情報配送方法及びその実施装置並びにその処理プログラムと記録媒体

(57) 【要約】

【課題】 マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能な技術を提供する。

【解決手段】 コンテンツを暗号化または復号化する為の鍵をユニキャストで各情報利用端末に配送するステップと、前記ユニキャストで配送された鍵を情報利用端末で取得するステップと、前記取得した鍵を当該情報利用端末に保存するステップと、情報提供端末に保存した鍵によりコンテンツを暗号化するステップと、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するステップと、前記マルチキャストで配送された暗号化コンテンツを情報利用端末で取得するステップと、前記取得した暗号化コンテンツを当該情報利用端末に保存した鍵で復号化するステップと、前記復号化したコンテンツを再生するステップとを有するものである。

図 1



【特許請求の範囲】

【請求項 1】 コンテンツをマルチキャストで情報提供端末から情報利用端末に配送する情報配送方法において、

コンテンツを暗号化または復号化する為の鍵を鍵提供端末で生成するステップと、前記生成した鍵をユニキャストで情報提供端末及び各情報利用端末に配送するステップと、前記ユニキャストで配送された鍵を情報提供端末で取得するステップと、前記取得した鍵を当該情報提供端末に保存するステップと、前記ユニキャストで配送された鍵を情報利用端末で取得するステップと、前記取得した鍵を当該情報利用端末に保存するステップと、前記情報提供端末に保存した鍵によりコンテンツを暗号化するステップと、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するステップと、前記マルチキャストで配送された暗号化コンテンツを情報利用端末で取得するステップと、前記取得した暗号化コンテンツを当該情報利用端末に保存した鍵で復号化するステップと、前記復号化したコンテンツを再生するステップとを有することを特徴とする情報配送方法。

【請求項 2】 前記生成した鍵にそれらの鍵を識別する為の識別情報を付加するステップと、鍵の配送完了を示す鍵配送完了通知を受けて次の暗号化処理で使用する鍵の識別情報を指定するステップと、前記指定された識別情報を持つ鍵を用いてコンテンツを暗号化するステップと、前記取得した暗号化コンテンツの暗号化で用いられた鍵の識別情報を確認するステップと、前記確認された識別情報に対応する鍵で暗号化コンテンツを復号化するステップとを有することを特徴とする請求項 1 に記載された情報配送方法。

【請求項 3】 新規の鍵の取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信するステップと、前記マルチキャストで送信された鍵更新広報を取得し、新規の鍵の配送を要求するステップとを有することを特徴とする請求項 1 または請求項 2 のいずれかに記載された情報配送方法。

【請求項 4】 鍵の配送の際に I P s e c の機能を利用することを特徴とする請求項 1 乃至請求項 3 のいずれか 1 項に記載された情報配送方法。

【請求項 5】 コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を情報利用端末から送信するステップと、前記送信された加入要求を受け付けるステップと、前記加入要求の受付が行われた利用者の情報利用端末に対して暗号化コンテンツを復号化する為の鍵を配送するステップとを有することを特徴とする請求項 1 乃至請求項 4 のいずれか 1 項に記載された情報配送方法。

【請求項 6】 前記加入要求を送信した利用者の利用資

格が発生する日時を示す加入日時をデータベースに格納するステップと、現在の日時と前記データベースに格納した加入日時との差が所定の時間以内であるかまたは現在の日時が前記加入日時を経過している場合に、当該加入日時に対応する利用者の情報利用端末に暗号化コンテンツを復号化する為の鍵を配送するステップとを有することを特徴とする請求項 5 に記載された情報配送方法。

【請求項 7】 前記送信された加入要求が受け付けられたことを示す加入要求応答を、当該加入要求を送信した情報利用端末へ通知するステップを有することを特徴とする請求項 5 または請求項 6 のいずれかに記載された情報配送方法。

【請求項 8】 前記配送先リストからの脱退要求を情報利用端末から送信するステップと、前記送信された脱退要求を受け付けるステップと、前記脱退要求の受付が行われた利用者の情報利用端末に対する前記鍵の配送を抑止するステップとを有することを特徴とする請求項 1 乃至請求項 7 のいずれか 1 項に記載された情報配送方法。

【請求項 9】 前記脱退要求を送信した利用者の利用資格が抹消される日時を示す脱退日時をデータベースに格納するステップと、現在の日時が前記脱退日時を経過しているかまたは次配送の鍵が脱退日時以降のコンテンツに相当する鍵である場合に、当該脱退日時に対応する利用者の情報利用端末への前記鍵の配送を抑止するステップとを有することを特徴とする請求項 8 に記載された情報配送方法。

【請求項 10】 前記送信された脱退要求が受け付けられたことを示す脱退要求応答を、当該脱退要求を送信した情報利用端末へ通知するステップを有することを特徴とする請求項 8 または請求項 9 のいずれかに記載された情報配送方法。

【請求項 11】 コンテンツを暗号化または復号化する為の鍵を提供する鍵提供端末において、コンテンツを暗号化または復号化する為の鍵を生成する鍵生成部と、情報提供端末及び情報提供端末から配送されるコンテンツの利用資格を持つ利用者の情報利用端末に前記生成した鍵をユニキャストで配送する鍵配送部とを備えることを特徴とする鍵提供端末。

【請求項 12】 コンテンツをマルチキャストで情報利用端末に提供する情報提供端末において、コンテンツを暗号化または復号化する為の鍵を生成する鍵生成部と、前記生成した鍵を保存する鍵保存部と、情報提供端末から配送されるコンテンツの利用資格を持つ利用者の情報利用端末に前記生成した鍵をユニキャストで配送する鍵配送部と、

前記保存した鍵によりコンテンツを暗号化するコンテンツ暗号化部と、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するコンテンツ配送部とを備えることを特徴とする情報提供端末。

10

20

30

40

50

3

【請求項 13】 前記生成した鍵にそれらの鍵を識別する為の識別情報を付加する識別情報付加部と、前記鍵配送部から鍵の配送完了を示す鍵配送完了通知を受けて次の暗号化処理で使用する鍵の識別情報を指定する鍵更新部とを備えることを特徴とする請求項 11 または請求項 12 のいずれかに記載された端末装置。

【請求項 14】 新規の鍵の取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信する鍵更新広報部を備えることを特徴とする請求項 11 乃至請求項 13 のいずれか 1 項に記載された端末装置。

【請求項 15】 鍵の配送の際に I P s e c の機能を利用することを特徴とする請求項 11 乃至請求項 14 のいずれか 1 項に記載された端末装置。

【請求項 16】 コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を情報利用端末から受付ける加入要求受付部を備え、前記鍵配送部は、前記加入要求の受付が行われた利用者の情報利用端末に対して暗号化コンテンツを復号化する為の鍵を配送するものであることを特徴とする請求項 11 乃至請求項 15 のいずれか 1 項に記載された端末装置。

【請求項 17】 前記加入要求を送信した利用者の利用資格が発生する日時を示す加入日時をデータベースに格納するデータベース部を備え、前記鍵配送部は、現在の日時と前記データベースに格納した加入日時との差が所定の時間以内であるかまたは現在の日時が前記加入日時を経過している場合に、当該加入日時に対応する利用者の情報利用端末に暗号化コンテンツを復号化する為の鍵を配送するものであることを特徴とする請求項 16 に記載された端末装置。

【請求項 18】 前記送信された加入要求が受け付けられたことを示す加入要求応答を、当該加入要求を送信した情報利用端末へ通知する加入要求応答部を備えることを特徴とする請求項 16 または請求項 17 のいずれかに記載された端末装置。

【請求項 19】 前記配送先リストからの脱退要求を情報利用端末から受付ける脱退要求受付部を備え、前記鍵配送部は、前記脱退要求の受付が行われた利用者の情報利用端末に対する前記鍵の配送を抑止するものであることを特徴とする請求項 11 乃至請求項 18 のいずれか 1 項に記載された端末装置。

【請求項 20】 前記データベース部は、前記脱退要求を送信した利用者の利用資格が抹消される日時を示す脱退日時をデータベースに格納し、前記鍵配送部は、現在の日時が前記脱退日時を経過しているかまたは次配送の鍵が脱退日時以降のコンテンツに相当する鍵である場合に、当該脱退日時に対応する利用者の情報利用端末への前記鍵の配送を抑止するものであることを特徴とする請求項 19 に記載された端末装置。

【請求項 21】 前記送信された脱退要求が受け付けられたことを示す脱退要求応答を、当該脱退要求を送信した

4

情報利用端末へ通知する脱退要求応答部を備えることを特徴とする請求項 19 または請求項 20 のいずれかに記載された端末装置。

【請求項 22】 コンテンツをマルチキャストで情報利用端末に提供する情報提供端末において、利用資格を持つ利用者の情報利用端末に配送されるコンテンツを暗号化する為の鍵を鍵提供端末からユニキャストで取得する鍵取得部と、前記取得した鍵を保存する鍵保存部と、前記保存した鍵によりコンテンツを暗号化するコンテンツ暗号化部と、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するコンテンツ配送部とを備えることを特徴とする情報提供端末。

【請求項 23】 マルチキャストで情報提供端末から配送されたコンテンツを取得する情報利用端末において、利用資格を持つ利用者の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を鍵提供端末からユニキャストで取得する鍵取得部と、前記取得した鍵を保存する鍵保存部と、

暗号化されたコンテンツである暗号化コンテンツを情報提供端末からマルチキャストで取得するコンテンツ取得部と、前記取得した暗号化コンテンツを前記保存した鍵で復号化するコンテンツ復号化部と、前記復号化したコンテンツを再生するコンテンツ再生部とを備えることを特徴とする情報利用端末。

【請求項 24】 前記取得した暗号化コンテンツの暗号化で用いられた鍵の識別情報を確認する識別情報確認部を備え、前記確認された識別情報に対応する鍵で暗号化コンテンツを復号化することを特徴とする請求項 23 に記載された情報利用端末。

【請求項 25】 新規の鍵の取得を促す鍵更新広報を取得し、新規の鍵の配送を要求する鍵更新情報取得部を備えることを特徴とする請求項 23 または請求項 24 のいずれかに記載された情報利用端末。

【請求項 26】 コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を送信する加入要求部を備えることを特徴とする請求項 23 乃至請求項 25 のいずれか 1 項に記載された情報利用端末。

【請求項 27】 前記送信した加入要求が受け付けられたことを示す加入要求応答を受信する加入要求応答受付部を備えることを特徴とする請求項 26 に記載された情報利用端末。

【請求項 28】 前記配送先リストからの脱退要求を送信する脱退要求部を備えることを特徴とする請求項 23 乃至請求項 27 のいずれか 1 項に記載された情報利用端末。

【請求項 29】 前記送信した脱退要求が受け付けられたことを示す脱退要求応答を受信する脱退要求応答受付部を備えることを特徴とする請求項 28 に記載された情報利用端末。

【請求項 30】 コンテンツを暗号化または復号化する為の鍵を提供する鍵提供端末としてコンピュータを機能させる為のプログラムにおいて、

コンテンツを暗号化または復号化する為の鍵を生成する鍵生成部と、情報提供端末及び情報提供端末から配送されるコンテンツの利用資格を持つ利用者の情報利用端末に前記生成した鍵をユニキャストで配送する鍵配送部としてコンピュータを機能させることを特徴とするプログラム。

【請求項 31】 コンテンツをマルチキャストで情報利用端末に提供する情報提供端末としてコンピュータを機能させる為のプログラムにおいて、

コンテンツを暗号化または復号化する為の鍵を生成する鍵生成部と、前記生成した鍵を保存する鍵保存部と、情報提供端末から配送されるコンテンツの利用資格を持つ利用者の情報利用端末に前記生成した鍵をユニキャストで配送する鍵配送部と、

前記保存した鍵によりコンテンツを暗号化するコンテンツ暗号化部と、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するコンテンツ配送部としてコンピュータを機能させることを特徴とするプログラム。

【請求項 32】 前記生成した鍵にそれらの鍵を識別する為の識別情報を付加する識別情報付加部と、前記鍵配送部から鍵の配送完了を示す鍵配送完了通知を受けて次の暗号化処理で使用する鍵の識別情報を指定する鍵更新部としてコンピュータを機能させることを特徴とする請求項 30 または請求項 31 のいずれかに記載されたプログラム。

【請求項 33】 新規の鍵の取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信する鍵更新広報部としてコンピュータを機能させることを特徴とする請求項 30 乃至請求項 32 のいずれか 1 項に記載されたプログラム。

【請求項 34】 鍵の配送の際に I P s e c の機能を利用することを特徴とする請求項 30 乃至請求項 33 のいずれか 1 項に記載されたプログラム。

【請求項 35】 コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を情報利用端末から受付ける加入要求受付部と、前記加入要求の受付が行われた利用者の情報利用端末に対して暗号化コンテンツを復号化する為の鍵を配送する鍵配送部としてコンピュータを機能させることを特徴とする請求項 30 乃至請求項 34 のいずれか 1 項に記載されたプログラム。

【請求項 36】 前記加入要求を送信した利用者の利用資格が発生する日時を示す加入日時をデータベースに格納するデータベース部と、現在の日時と前記データベースに格納した加入日時との差が所定の時間以内であるかまたは現在の日時が前記加入日時を経過している場合に、当該加入日時に対応する利用者の情報利用端末に暗

号化コンテンツを復号化する為の鍵を配送する鍵配送部としてコンピュータを機能させることを特徴とする請求項 35 に記載されたプログラム。

【請求項 37】 前記送信された加入要求が受け付けられたことを示す加入要求応答を、当該加入要求を送信した情報利用端末へ通知する加入要求応答部としてコンピュータを機能させることを特徴とする請求項 35 または請求項 36 のいずれかに記載されたプログラム。

【請求項 38】 前記配送先リストからの脱退要求を情報利用端末から受付ける脱退要求受付部と、前記脱退要求の受付が行われた利用者の情報利用端末に対する前記鍵の配送を抑止する鍵配送部としてコンピュータを機能させることを特徴とする請求項 30 乃至請求項 37 のいずれか 1 項に記載されたプログラム。

【請求項 39】 前記データベース部は、前記脱退要求を送信した利用者の利用資格が抹消される日時を示す脱退日時をデータベースに格納し、前記鍵配送部は、現在の日時が前記脱退日時を経過しているかまたは次配送の鍵が脱退日時以降のコンテンツに相当する鍵である場合に、当該脱退日時に対応する利用者の情報利用端末への前記鍵の配送を抑止するものであることを特徴とする請求項 38 に記載されたプログラム。

【請求項 40】 前記送信された脱退要求が受け付けられたことを示す脱退要求応答を、当該脱退要求を送信した情報利用端末へ通知する脱退要求応答部としてコンピュータを機能させることを特徴とする請求項 38 または請求項 39 のいずれかに記載されたプログラム。

【請求項 41】 コンテンツをマルチキャストで情報利用端末に提供する情報提供端末としてコンピュータを機能させる為のプログラムにおいて、

利用資格を持つ利用者の情報利用端末に配送されるコンテンツを暗号化する為の鍵を鍵提供端末からユニキャストで取得する鍵取得部と、前記取得した鍵を保存する鍵保存部と、

前記保存した鍵によりコンテンツを暗号化するコンテンツ暗号化部と、前記暗号化したコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送するコンテンツ配送部としてコンピュータを機能させることを特徴とするプログラム。

【請求項 42】 マルチキャストで情報提供端末から配送されたコンテンツを取得する情報利用端末としてコンピュータを機能させる為のプログラムにおいて、

利用資格を持つ利用者の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を鍵提供端末からユニキャストで取得する鍵取得部と、前記取得した鍵を保存する鍵保存部と、

暗号化されたコンテンツである暗号化コンテンツを情報提供端末からマルチキャストで取得するコンテンツ取得部と、前記取得した暗号化コンテンツを前記保存した鍵で復号化するコンテンツ復号化部と、前記復号化したコ

ンテンツを再生するコンテンツ再生部としてコンピュータを機能させることを特徴とするプログラム。

【請求項43】 前記取得した暗号化コンテンツの暗号化で用いられた鍵の識別情報を確認する識別情報確認部と、前記確認された識別情報に対応する鍵で暗号化コンテンツを復号化するコンテンツ復号化部としてコンピュータを機能させることを特徴とする請求項42に記載されたプログラム。

【請求項44】 新規の鍵の取得を促す鍵更新広報を取得し、新規の鍵の配送を要求する鍵更新情報取得部としてコンピュータを機能させることを特徴とする請求項42または請求項43のいずれかに記載されたプログラム。

【請求項45】 コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を送信する加入要求部としてコンピュータを機能させることを特徴とする請求項42乃至請求項44のいずれか1項に記載されたプログラム。

【請求項46】 前記送信した加入要求が受け付けられたことを示す加入要求応答を受信する加入要求応答受付部としてコンピュータを機能させることを特徴とする請求項45に記載されたプログラム。

【請求項47】 前記配送先リストからの脱退要求を送信する脱退要求部としてコンピュータを機能させることを特徴とする請求項42乃至請求項46のいずれか1項に記載されたプログラム。

【請求項48】 前記送信した脱退要求が受け付けられたことを示す脱退要求応答を受信する脱退要求応答受付部としてコンピュータを機能させることを特徴とする請求項47に記載されたプログラム。

【請求項49】 請求項30乃至請求項48のいずれか1項のプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はコンテンツをマルチキャストで配送する情報配送システムに関し、特にストリームコンテンツを暗号化した暗号化コンテンツをマルチキャストで配送し、ユニキャストで配送された復号鍵で復号化することにより情報の利用制御を可能とし、利用者の加入及び脱退に応じて復号鍵の配送先を管理する情報配送システムに適用して有効な技術に関するものである。

【0002】

【従来の技術】従来、複数の利用者に対してストリームコンテンツ等の同一のコンテンツを提供する場合、マルチキャストを用いることにより効率良くコンテンツの配送を行うことができる。このマルチキャストを用いたコンテンツの配送では、利用者がマルチキャストアドレスを指定することにより、誰でも簡単にそのコンテンツを

利用することができる。

【0003】また前記マルチキャストを用いて、利用資格を有する特定の利用者向けにコンテンツを提供しようとする場合には、そのコンテンツを利用者のみが復号できる状態で（例えば利用者に予め配られている鍵を利用する等）暗号化し、その暗号化コンテンツをマルチキャストで配送するという手法がある。利用者は、マルチキャストアドレスを指定して受信した暗号化コンテンツを、予め配られている鍵で復号化することにより、そのコンテンツを利用することができる。

【0004】

【発明が解決しようとする課題】前記従来技術でマルチキャストを用いて暗号化すること無くコンテンツの配送を行った場合、マルチキャストアドレスを指定すれば誰でも簡単にそのストリームコンテンツを利用できる為、利用資格を有する特定の利用者向けにコンテンツを提供しようとした場合、前記暗号化を用いないマルチキャストではコンテンツの不正利用が行われるという問題があった。

【0005】またストリームコンテンツを暗号化した暗号化コンテンツをマルチキャストで配送した場合、盗聴によるストリームコンテンツの不正利用は防御しているが、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能な為、不正利用される恐れがあるという問題があった。

【0006】本発明の目的は上記問題を解決し、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能であると言う従来の問題点を解決し、マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能な技術を提供することにある。

【0007】

【課題を解決するための手段】本発明は、コンテンツをマルチキャストで情報提供端末から情報利用端末に配送する情報配送システムにおいて、マルチキャストで情報提供端末から各情報利用端末に配送された暗号化コンテンツを、ユニキャストで当該情報利用端末に配送された鍵によって復号化するものである。

【0008】本発明は、ストリームコンテンツ等を暗号化した暗号化コンテンツに対応する鍵をユニキャストで利用資格を持つ利用者に配送して更新することによって、マルチキャストストリームコンテンツを安全に配送すると共に、利用者の利用資格の更新を可能にすることを主な特徴とする。

【0009】本発明の情報提供端末では以下の様にストリームコンテンツ等のコンテンツの暗号化及び配送を行なう。まず鍵提供端末の鍵生成部は、ストリームコンテンツCの暗号化または復号化に利用する暗号鍵Kを生成する。暗号鍵Kには鍵が一意に定まる様な識別情報iを予め与えておくものとし、生成した暗号鍵Kiを鍵配送

部に送付する。

【0010】鍵配送部は、送付された暗号鍵*K_i*を、情報提供端末及び現在の利用資格保持者集合*G*の各情報利用端末にユニキャストで配送する。情報提供端末及び利用資格保持者集合*G*の各情報利用端末に暗号鍵*K_i*の配送を終了したら、配送が終了したことを鍵配送部から鍵更新部に知らせ、鍵更新部はコンテンツ暗号化部に送信が終了した鍵を通知する。また鍵提供端末は所定の時間間隔が経過した場合等、所定の条件で次の鍵の生成して配送するものとしても良い。鍵の配送においては先にマルチキャストで鍵の更新を呼びかけ、各情報利用端末からユニキャストで鍵を取得しても構わないものとする。

【0011】コンテンツ暗号化部は、鍵更新部から暗号鍵*K_i*の配送終了通知を受け取ったら、次パケットから暗号鍵*K_i*を利用して暗号化を行って暗号化コンテンツ*K_i(C)*を生成し、暗号化に使った鍵の識別情報*i*を暗号化コンテンツ*K_i(C)*に付加する。更に暗号化コンテンツ*K_i(C)*をコンテンツ配送部に送付し、コンテンツ配送部は暗号化コンテンツ*K_i(C)*をマルチキャストで送付する。

【0012】情報利用端末では以下の様にコンテンツの復号化及び再生を行う。まず鍵取得部は、鍵提供端末からユニキャストで送付される暗号鍵*K_i*を受け取る。或いはマルチキャストで鍵更新の情報を鍵提供端末から取得したら各情報利用端末からユニキャストで暗号鍵*K_i*の取得を行なう。受け取った暗号鍵*K_i*を鍵保存部により保存した後、コンテンツ取得部は、情報提供端末からマルチキャストで送付される暗号化コンテンツ*K_i*

(*C*)を受け取る。コンテンツ復号化部は、送付された暗号化コンテンツ*K_i(C)*から鍵の識別情報*i*を取り出し、その識別情報*i*に合った暗号鍵*K_i*を鍵保存部から取得し、この暗号鍵*K_i*を利用してコンテンツの復号化を行なう。コンテンツ再生部は、復号化したコンテンツの再生を行なう。

【0013】鍵提供端末が所定の条件で鍵を生成して更新していくことによって、コンテンツをマルチキャストで配送しても利用資格保持者以外がコンテンツを利用することは不可能になり、また利用資格を失った利用者が長時間に渡ってコンテンツを不正利用し続けることを防止することができる。

【0014】また本発明の鍵提供端末では、復号鍵の生成・管理及び配送先リストの管理を行ない、鍵提供端末で復号鍵の利用者リスト即ち配送先リストを管理することにより、その時点での利用者のみマルチキャストストリームコンテンツの利用を可能にする。鍵提供端末は、利用者が配送先リストに加入を行なう加入処理と利用者が資格を失う或いは意図的に配送先リストから脱退する脱退処理を管理することにより、利用者の管理を行なう。

【0015】加入処理において、鍵提供端末と情報利用

端末間では以下の処理が行なわれる。情報利用端末は、加入要求部を通じて鍵提供端末の加入要求受付部に対して加入要求を送付する。また情報利用端末は、加入したいチャンネルの情報（コンテンツの名称、コンテンツの識別情報、マルチキャストアドレス等）や加入日時情報等を鍵提供端末に送付するものとする。

【0016】鍵提供端末は、情報利用端末から送信された加入日時情報等をデータベースに格納しておき、現在の日時と前記データベースに格納した加入日時との差が所定の時間以内であるかまたは現在の日時が前記加入日時を経過している場合に、当該加入日時に対応する利用者の情報利用端末に、要求されているコンテンツに対応する復号鍵をユニキャストで送付する。ここで、対象者に対し鍵配送の準備が整ったという情報を鍵更新広報部から送付し、この情報を取得した利用状態にある情報利用端末はユニキャストで鍵情報を鍵提供端末から取得しても良い。

【0017】以降、該当コンテンツに対応する復号鍵が更新された場合、鍵提供端末はデータベース部のデータを参照し該当する情報利用端末に更新された復号鍵をユニキャストで送付する。

【0018】脱退処理において、鍵提供端末と情報利用端末間では以下の処理が行なわれる。情報利用端末は、脱退要求部を通じて、鍵提供端末の脱退要求受付部に対して脱退要求を送付する。また情報利用端末は、脱退したいチャンネルの情報や脱退日時情報等を鍵提供端末に送付する。

【0019】鍵提供端末は、情報利用端末から送信された脱退日時情報等をデータベースに格納しておき、現在の日時が前記脱退日時を経過しているかまたは次配送の鍵が脱退日時以降のコンテンツに相当する鍵である場合に、当該脱退日時に対応する利用者の情報利用端末への、要求されているコンテンツに対応する復号鍵の送付を取り止める。

【0020】所定時間毎に鍵を生成して更新していき、鍵提供端末を利用して利用者の加入と脱退を管理して復号鍵をユニキャストで配送することにより、マルチキャストで暗号化コンテンツを配送しても利用者以外にコンテンツを利用することは不可能になり、また利用資格を失った利用者が長期に渡ってコンテンツを不正利用し続けることを防止することができる。

【0021】以上の様に本発明の情報配送システムによれば、マルチキャストで情報提供端末から各情報利用端末に配送された暗号化コンテンツを、ユニキャストで当該情報利用端末に配送された鍵によって復号化するので、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能であると言う従来の問題点を解決し、マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能である。

【0022】

【発明の実施の形態】（実施形態1）以下に鍵をユニキャストで配送した後にストリームコンテンツをマルチキャストで配送する実施形態1の情報配送システムについて説明する。

【0023】図1は本実施形態の情報配送システムの概略構成を示す図である。図1に示す様に本実施形態の情報配送システムは、情報提供端末1と、情報利用端末2～4と、鍵提供端末5とを有している。

【0024】情報提供端末1は、ストリームコンテンツをマルチキャストで情報利用端末2～4に配送する装置である。情報利用端末2～4は、マルチキャストで情報提供端末1から配送されたストリームコンテンツを取得する装置である。鍵提供端末5は、ストリームコンテンツを暗号化または復号化する為の鍵をユニキャストで情報提供端末1及び情報利用端末2～4に配送する装置である。

【0025】本実施形態において、情報提供端末1と情報利用端末2～4と鍵提供端末5は、それぞれインターネットに接続されており、ネットワーク上でマルチキャストとユニキャストの通信が可能であるものとする。本実施形態では、ストリームコンテンツをマルチキャストで情報利用端末2～4に配送する情報提供端末1と、そのストリームコンテンツを暗号化または復号化する為の鍵を配送する鍵提供端末5とが別装置であるものとして説明するが、両者を同一の装置で実現しても良い。

【0026】図2は本実施形態の情報提供端末1の概略構成を示す図である。図2に示す様に本実施形態の情報提供端末1は、CPU201と、メモリ202と、磁気ディスク装置203と、入力装置204と、出力装置205と、CD-ROM装置206と、通信装置207とを有している。

【0027】CPU201は、情報提供端末1全体の動作を制御する装置である。メモリ202は、情報提供端末1全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置203は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【0028】入力装置204は、ストリームコンテンツをマルチキャストで各情報利用端末へ配送する為の各種入力を行う装置である。出力装置205は、ストリームコンテンツの配送に伴う各種出力を行う装置である。

【0029】CD-ROM装置206は、前記各種処理プログラムを記録したCD-ROMの内容を読み出す装置である。通信装置207は、インターネットやイントラネット等のネットワークを介して各情報利用端末及び鍵提供端末5との通信を行う装置である。

【0030】また情報提供端末1は、鍵取得部211と、鍵保存部212と、コンテンツ暗号化部213と、コンテンツ配送部214とを有している。

【0031】鍵取得部211は、利用資格を持つ利用者の情報利用端末に配送されるコンテンツを暗号化する為の鍵を鍵提供端末5からユニキャストで取得する処理部である。鍵保存部212は、鍵取得部211によって取得された鍵をメモリ202または磁気ディスク装置203に保存する処理部である。

【0032】コンテンツ暗号化部213は、鍵保存部212によってメモリ202または磁気ディスク装置203に保存された鍵によりコンテンツを暗号化する処理部である。コンテンツ配送部214は、コンテンツ暗号化部213によって暗号化されたコンテンツである暗号化コンテンツをマルチキャストで各情報利用端末に配送する処理部である。

【0033】情報提供端末1を鍵取得部211、鍵保存部212、コンテンツ暗号化部213及びコンテンツ配送部214として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0034】図3は本実施形態の情報利用端末2の概略構成を示す図である。図3に示す様に本実施形態の情報利用端末2は、CPU301と、メモリ302と、磁気ディスク装置303と、入力装置304と、出力装置305と、CD-ROM装置306と、通信装置307とを有している。

【0035】CPU301は、情報利用端末2全体の動作を制御する装置である。メモリ302は、情報利用端末2全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置303は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【0036】入力装置304は、マルチキャストで情報提供端末1から配送されたストリームコンテンツを取得する為の各種入力を行う装置である。出力装置305は、ストリームコンテンツの取得に伴う各種出力を行う装置である。

【0037】CD-ROM装置306は、前記各種処理プログラムを記録したCD-ROMの内容を読み出す装置である。通信装置307は、インターネットやイントラネット等のネットワークを介して情報提供端末1及び鍵提供端末5との通信を行う装置である。

【0038】また情報利用端末2は、鍵取得部311と、鍵保存部312と、コンテンツ取得部313と、コンテンツ復号化部314と、コンテンツ再生部315とを有している。

【0039】鍵取得部311は、利用資格を持つ利用者

の情報利用端末に配送された暗号化コンテンツを復号化する為の鍵を鍵提供端末5からユニキャストで取得する処理部である。鍵保存部312は、鍵取得部311によって取得された鍵をメモリ302または磁気ディスク装置303に保存する処理部である。

【0040】コンテンツ取得部313は、暗号化コンテンツを情報提供端末1からマルチキャストで取得する処理部である。コンテンツ復号化部314は、コンテンツ取得部313によって取得された暗号化コンテンツを、鍵保存部312によってメモリ302または磁気ディスク装置303に保存された鍵で復号化する処理部である。コンテンツ再生部315は、コンテンツ復号化部314によって復号化されたコンテンツを再生する処理部である。

【0041】情報利用端末2を鍵取得部311、鍵保存部312、コンテンツ取得部313、コンテンツ復号化部314及びコンテンツ再生部315として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0042】なお情報利用端末3及び4についても情報利用端末2の構成と同様であるものとする。

【0043】図4は本実施形態の鍵提供端末5の概略構成を示す図である。図4に示す様に本実施形態の鍵提供端末5は、CPU401と、メモリ402と、磁気ディスク装置403と、入力装置404と、出力装置405と、CD-ROM装置406と、通信装置407とを有している。

【0044】CPU401は、鍵提供端末5全体の動作を制御する装置である。メモリ402は、鍵提供端末5全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置403は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【0045】入力装置404は、コンテンツを暗号化または復号化する為の鍵をユニキャストで情報提供端末1及び各情報利用端末へ配送する為の各種入力を行う装置である。出力装置405は、コンテンツを暗号化または復号化する為の鍵の配送に伴う各種出力を行う装置である。

【0046】CD-ROM装置406は、前記各種処理プログラムを記録したCD-ROMの内容を読み出す装置である。通信装置407は、インターネットやイントラネット等のネットワークを介して情報提供端末1及び各情報利用端末との通信を行う装置である。

【0047】また鍵提供端末5は、鍵生成部411と、鍵配送部412とを有している。

【0048】鍵生成部411は、コンテンツを暗号化または復号化する為の鍵を生成する処理部である。鍵配送部412は、情報提供端末1及び情報提供端末1から配送されるコンテンツの利用資格を持つ利用者の情報利用端末に鍵生成部411によって生成された鍵をユニキャストで配送する処理部である。

【0049】鍵提供端末5を鍵生成部411及び鍵配送部412として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0050】なおコンテンツを暗号化または復号化する為の鍵の生成及び配送を階層化された複数の鍵提供端末5によって行い、処理負荷を分散させても良い。

【0051】本実施形態の情報提供端末1では、配送対象のストリームコンテンツが保存されているか、或いはリアルタイムでストリームコンテンツが取得されるものとし、このストリームコンテンツを情報提供端末1から情報利用端末2～4に配送して再生する際の例について説明する。なおこの例ではコンテンツの暗号化に利用される暗号鍵は復号鍵を兼ねているものとするが、公開鍵暗号方式の様に暗号鍵と復号鍵とが異なるものとしても良く、暗号鍵と復号鍵とが異なるものとした場合には、情報提供端末1に暗号鍵を配送し、コンテンツの利用資格を持つ利用者の情報利用端末には復号鍵の配送を行うものとする。

【0052】図5は本実施形態の鍵提供端末5の鍵配送処理の処理手順を示すフローチャートである。図5に示す様に鍵提供端末5の鍵生成部411は、ストリームコンテンツであるコンテンツCを暗号化または復号化する為の暗号鍵Kを生成し、鍵配送部412は、情報提供端末1及び情報提供端末1から配送されるコンテンツの利用資格を持つ利用者の情報利用端末に前記生成された鍵をユニキャストで配送する処理を行う。

【0053】図5のステップ501で鍵提供端末5の鍵生成部411は、コンテンツCを暗号化する為の暗号鍵Kを生成して鍵配送部412へ渡す。ステップ502で鍵配送部412は、前記生成された暗号鍵Kをユニキャストで情報提供端末1へ配送する。ここで配送の際にIPsec(IP security protocol)等を用いて通信路をセキュアな状態に保つても構わないものとする。

【0054】ステップ503で鍵配送部412は、情報提供端末1の利用資格者DBの内容を参照し、情報提供端末1から配送されるコンテンツCの利用資格を持つ利

用者について、その情報利用端末のIPアドレスを読み出す。

【0055】ステップ504では、前記読み出した情報利用端末のIPアドレスを宛先としたユニキャストによって暗号鍵Kを配送する。ここで配送の際にIPsec等を用いて通信路をセキュアな状態に保っても構わないものとする。

【0056】ステップ505では、前記利用資格を持つ全ての利用者の情報利用端末に暗号鍵Kを配送したかどうかを調べ、まだ配送を行っていない情報利用端末がある場合にはステップ503へ戻って暗号鍵Kの配送を続行し、利用資格を持つ全ての利用者の情報利用端末への配送を完了した場合には暗号鍵Kの配送処理を終了する。

【0057】図6は本実施形態の情報提供端末1または各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。図6に示す様に情報提供端末1の鍵取得部211は、鍵提供端末5からユニキャストで配送された暗号鍵Kを取得して、鍵保存部212によりその暗号鍵Kを保存する処理を行う。同様に各情報利用端末の鍵取得部311は、鍵提供端末5からユニキャストで配送された暗号鍵Kを取得して、鍵保存部312によりその暗号鍵Kを保存する処理を行う。

【0058】図6のステップ601で情報提供端末1の鍵取得部211は、鍵提供端末5からユニキャストで暗号鍵Kを受信しているかどうかを調べ、暗号鍵Kを受信している場合にはステップ602へ進み、前記受信した暗号鍵Kを取得してこれを鍵保存部212に渡す。ステップ603で鍵保存部212は、前記取得した暗号鍵Kをメモリ302または磁気ディスク装置303に保存する。

【0059】各情報利用端末の場合も同様に図6のステップ601で各情報利用端末の鍵取得部311は、鍵提供端末5からユニキャストで暗号鍵Kを受信しているかどうかを調べ、暗号鍵Kを受信している場合にはステップ602へ進み、前記受信した暗号鍵Kを取得してこれを鍵保存部312に渡す。ステップ603で鍵保存部312は、前記取得した暗号鍵Kをメモリ302または磁気ディスク装置303に保存する。ここで各情報利用端末が暗号鍵Kを磁気ディスク装置303に保存する場合には暗号鍵Kを暗号化して保存を行うものとする。

【0060】図7は本実施形態の情報提供端末1のコンテンツ配送処理の処理手順を示すフローチャートである。図7に示す様に情報提供端末1のコンテンツ暗号化部213は、鍵保存部212によって保存された暗号鍵Kを用いてコンテンツCを暗号化し、前記暗号化されたコンテンツである暗号化コンテンツK(C)をコンテンツ配送部214によりマルチキャストで各情報利用端末に配送する処理を行う。

【0061】図7のステップ701で情報提供端末1の

コンテンツ暗号化部213は、鍵保存部212によってメモリ202または磁気ディスク装置203に保存されていた暗号鍵Kを読み出す。ステップ702では、配送対象のコンテンツCを所定の単位で読み出し、ステップ703では、前記読み出したコンテンツCを暗号鍵Kで暗号化して暗号化コンテンツK(C)を生成し、コンテンツ配送部214に渡す。ここで暗号化の単位はネットワーク配送を行う為のケットの大きさ単位としても構わないものとする。またコンテンツの暗号化の際にコンテンツのスクランブル処理やハッシュ処理を併用しても良い。

【0062】ステップ704でコンテンツ配送部214は、前記生成された暗号化コンテンツK(C)をマルチキャストで情報利用端末2~4へ配送する。ステップ705では、配送対象のコンテンツCについて全てのデータを情報利用端末2~4に配送したかどうかを調べ、まだ配送を行っていないデータがある場合にはステップ702へ戻ってコンテンツCの配送を続行し、全データの配送を完了した場合にはコンテンツCの配送処理を終了する。

【0063】図8は本実施形態の各情報利用端末のコンテンツ利用処理の処理手順を示すフローチャートである。図8に示す様に各情報利用端末のコンテンツ取得部313は、暗号化コンテンツK(C)を情報提供端末1からマルチキャストで取得し、コンテンツ復号化部314は、前記取得した暗号化コンテンツK(C)を鍵保存部312によって保存されていた暗号鍵Kにより復号化し、前記復号化されたコンテンツCをコンテンツ再生部315により再生する処理を行う。

【0064】図8のステップ801で各情報利用端末のコンテンツ取得部313は、情報提供端末1からマルチキャストで暗号化コンテンツK(C)を受信しているかどうかを調べ、暗号化コンテンツK(C)を受信している場合にはステップ802へ進み、前記受信した暗号化コンテンツK(C)を取得してコンテンツ復号化部314に渡す。

【0065】ステップ803でコンテンツ復号化部314は、暗号鍵Kのメモリ302または磁気ディスク装置303からの読み込みが未実行であるかどうかを調べ、暗号鍵Kの読み込みが未実行である場合にはステップ804へ進む。ステップ804では、鍵保存部312によってメモリ302または磁気ディスク装置303に保存されている暗号鍵Kを読み出す。

【0066】ステップ805では、ステップ802で取得した暗号化コンテンツK(C)をステップ804で読み出した暗号鍵Kによって復号化してコンテンツCを生成する。ステップ806でコンテンツ再生部315は、前記復号化によって得られたコンテンツCを再生する。

【0067】前記の様に本実施形態では、情報提供端末1から配送されるコンテンツCの利用資格を持つ利用者

10

20

30

40

50

の情報利用端末へユニキャストで暗号鍵 K（復号兼用）を配送した後、暗号化コンテンツ K（C）をマルチキャストで各情報利用端末へ配送しているので、コンテンツの利用資格を失った利用者による不正利用を防止しつつマルチキャストを利用した効率的なコンテンツの提供を行うことができる。

【0068】以上説明した様に本実施形態の情報配送システムによれば、マルチキャストで情報提供端末から各情報利用端末に配送された暗号化コンテンツを、ユニキャストで当該情報利用端末に配送された鍵によって復号化するの、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能であると言う従来の問題点を解決し、マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能である。

【0069】（実施形態 2）以下に鍵を鍵提供端末から各情報利用端末へ配布して鍵の更新を行った後にストリームコンテンツをマルチキャストで配送する実施形態 2 の情報配送システムについて説明する。

【0070】図 9 は本実施形態の鍵提供端末 5 の概略構成を示す図である。図 9 に示す様に本実施形態の鍵提供端末 5 は、識別情報付加部 911 と、鍵更新部 912 とを有している。

【0071】識別情報付加部 911 は、前記生成した鍵にそれらの鍵を識別する為の識別情報を付加する処理部である。鍵更新部 912 は、鍵配送部 412 から鍵の配送完了を示す鍵配送完了通知を受けて次の暗号化処理で使用する鍵の識別情報を情報提供端末 1 に指定する処理部である。

【0072】鍵提供端末 5 を識別情報付加部 911 及び鍵更新部 912 として機能させる為のプログラムは、CD-ROM 等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体は CD-ROM 以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0073】本実施形態において、情報提供端末 1 は実施形態 1 と同様の構成であるものとし、情報提供端末 1 と情報利用端末 2～4 と鍵提供端末 5 は、実施形態 1 と同様にそれぞれインターネットに接続されており、ネットワーク上でマルチキャストとユニキャストの通信が可能であるものとする。本実施形態では、ストリームコンテンツをマルチキャストで情報利用端末 2～4 に配送する情報提供端末 1 と、そのストリームコンテンツを暗号化または復号化する為の鍵を配送する鍵提供端末 5 とが別装置であるものとして説明するが、両者を同一の装置で実現しても良い。

【0074】図 10 は本実施形態の情報利用端末 2 の概略構成を示す図である。図 10 に示す様に本実施形態の情報利用端末 2 は識別情報確認部 1011 を有している。識別情報確認部 1011 は、前記取得した暗号化コンテンツの暗号化で用いられた鍵の識別情報を確認する処理部である。

【0075】情報利用端末 2 を識別情報確認部 1011 として機能させる為のプログラムは、CD-ROM 等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体は CD-ROM 以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0076】なお情報利用端末 3 及び 4 についても情報利用端末 2 の構成と同様であるものとする。

【0077】本実施形態の情報提供端末 1 には、配送対象のストリームコンテンツが保存されているか、或いはリアルタイムでストリームコンテンツが取得されるものとし、鍵提供端末 5 から情報提供端末 1 及び各情報利用端末に鍵を、また情報提供端末 1 から各情報利用端末に暗号化コンテンツを送付し、各情報利用端末で暗号化コンテンツを復号化して再生する際の例について説明する。なおこの例ではコンテンツの暗号化に利用される暗号鍵は復号鍵を兼ねており、その鍵は所定の時間間隔で更新されるものとし、公開鍵暗号方式の様に暗号鍵と復号鍵とが異なるものとしても良く、暗号鍵と復号鍵とが異なるものとした場合には、情報提供端末 1 に暗号鍵を配送し、コンテンツの利用資格を持つ利用者の情報利用端末には復号鍵の配送を行うものとする。

【0078】図 11 は本実施形態の鍵提供端末 5 の鍵配送処理の処理手順を示すフローチャートである。図 11 に示す様に鍵提供端末 5 の鍵生成部 411 は、ストリームコンテンツであるコンテンツ C を暗号化または復号化する為の暗号鍵 K を生成し、前記生成された暗号鍵 K にその鍵を識別する為の識別情報 i を識別情報付加部 911 により付加する。また鍵配送部 412 により情報提供端末 1 及び各情報利用端末にその暗号鍵 K i をユニキャストで配送した後、次の暗号化処理で使用する鍵の識別情報 i を鍵更新部 912 により情報提供端末 1 に指定する処理を行う。

【0079】図 11 のステップ 1101 で鍵提供端末 5 の鍵生成部 411 は、所定の時間が経過した場合や情報提供端末 1 の利用資格者 DB 中の利用資格が変更された場合等の暗号鍵 K を生成する条件が成立したかどうかを調べ、暗号鍵 K を生成する条件が成立した場合にはステップ 1102 へ進む。

【0080】ステップ 1102 では、コンテンツ C を暗

号化する為の暗号鍵Kを生成する。暗号鍵Kとして通信時にIPsecで利用されているものを利用して構わないものとする。

【0081】ステップ1103で識別情報付加部911は、前記生成された暗号鍵Kに識別情報iを付加して鍵配送部412へ渡す。この識別情報はIPsecのSA (Security Association)に含まれる情報を利用して構わないものとする。

【0082】ステップ1104で鍵配送部412は、前記生成された暗号鍵Kiをユニキャストで情報提供端末1へ配送する。ここで配送の際にIPsec等を用いて通信路をセキュアな状態に保っても構わないものとする。

【0083】ステップ1105で鍵配送部412は、情報提供端末1の利用資格者DBの内容を参照し、情報提供端末1から配送されるコンテンツCの利用資格を持つ利用者について、その情報利用端末のIPアドレスを読み出す。

【0084】ステップ1106では、前記読み出した情報利用端末のIPアドレスを宛先としたユニキャストによって暗号鍵Kiを配送する。ここで配送の際にIPsec等を用いて通信路をセキュアな状態に保っても構わないものとする。

【0085】ステップ1107では、前記利用資格を持つ全ての利用者の情報利用端末に暗号鍵Kiを配送したかどうかを調べ、まだ配送を行っていない情報利用端末がある場合にはステップ1105へ戻って暗号鍵Kiの配送を続行し、利用資格を持つ全ての利用者の情報利用端末への配送を完了した場合にはステップ1108へ進む。ここで鍵の配送の完了とは、各情報利用端末と鍵提供端末5がユニキャストで鍵の通信を行って正常終了した場合の他に、情報利用端末2～4からの応答が無く、タイムアウトした場合を含んでいても構わないものとする。

【0086】ステップ1108では、利用資格を持った全ての利用者に対する暗号鍵Kiの配送が完了したことを示す鍵配送完了通知を鍵更新部912に伝え、ステップ1109で鍵更新部912は、配送が完了した暗号鍵Kiを次の暗号化処理で使用する鍵として決定し、その暗号鍵Kiの識別情報i或いは暗号鍵Kiそのものの情報を情報提供端末1のコンテンツ暗号化部213に通知してステップ1101へ戻る。

【0087】図12は本実施形態の情報提供端末1または各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。図12に示す様に情報提供端末1の鍵取得部211は、鍵提供端末5からユニキャストで配送された暗号鍵Kiを取得して、鍵保存部212によりその暗号鍵Kiを保存する処理を行う。同様に各情報利用端末の鍵取得部311は、鍵提供端末5からユニキャストで配送された暗号鍵Kiを取得して、鍵保存部312

によりその暗号鍵Kiを保存する処理を行う。

【0088】図12のステップ1201で情報提供端末1の鍵取得部211は、鍵提供端末5からユニキャストで暗号鍵Kiを受信しているかどうかを調べ、暗号鍵Kiを受信している場合にはステップ1202へ進み、前記受信した暗号鍵Kiを取得して鍵保存部212に渡す。

【0089】ステップ1203で鍵保存部212は、鍵提供端末5の識別情報付加部911によって付加された識別情報iを暗号鍵Kiから読み出し、ステップ1204では、ステップ1202で取得した暗号鍵Kiをステップ1203で読み出した識別情報i毎に分類してメモリ302または磁気ディスク装置303に保存する。

【0090】各情報利用端末の場合も同様に図12のステップ1201で各情報利用端末の鍵取得部311は、鍵提供端末5からユニキャストで暗号鍵Kiを受信しているかどうかを調べ、暗号鍵Kiを受信している場合にはステップ1202へ進み、前記受信した暗号鍵Kiを取得して鍵保存部312に渡す。

【0091】ステップ1203で鍵保存部312は、鍵提供端末5の識別情報付加部911によって付加された識別情報iを暗号鍵Kiから読み出し、ステップ1204では、ステップ1202で取得した暗号鍵Kiをステップ1203で読み出した識別情報i毎に分類してメモリ302または磁気ディスク装置303に保存する。ここで各情報利用端末が暗号鍵Kiを磁気ディスク装置303に保存する場合には暗号鍵Kiを暗号化して保存を行うものとする。

【0092】図13は本実施形態の情報提供端末1のコンテンツ配送処理の処理手順を示すフローチャートである。図13に示す様に情報提供端末1のコンテンツ暗号化部213は、鍵保存部212によって保存された鍵の内、鍵提供端末5の鍵更新部912により指定された識別情報iの暗号鍵Kiを用いてコンテンツCを暗号化し、前記暗号化されたコンテンツである暗号化コンテンツKi(C)をコンテンツ配送部214によりマルチキャストで各情報利用端末に配送する処理を行う。

【0093】図13のステップ1301で情報提供端末1のコンテンツ暗号化部213は、鍵保存部212によってメモリ202または磁気ディスク装置203に保存されていた鍵の内、鍵提供端末5の鍵更新部912により指定された識別情報iの暗号鍵Kiを読み出す。

【0094】ステップ1302では、配送対象のコンテンツCを所定の単位で読み出し、ステップ1303では、ステップ1302で読み出したコンテンツCのデータをステップ1301で読み出した暗号鍵Kiで暗号化して暗号化コンテンツKi(C)を生成し、コンテンツ配送部214に渡す。ここで暗号化の単位はネットワーク配送を行う為のパケットの大きさを単位としても構わないものとする。またコンテンツの暗号化の際にコンテ

ツのスクランブル処理やハッシュ処理を併用しても良い。

【0095】ステップ1304でコンテンツ配送部214は、前記生成された暗号化コンテンツ K_i (C)のヘッダー等に暗号鍵 K_i の識別情報 i を付加する。なおここでIPsecのヘッダーを利用しても構わないものとする。

【0096】ステップ1305では、前記識別情報 i の付加された暗号化コンテンツ K_i (C)をマルチキャストで情報利用端末2~4へ配送する。ステップ1306では、配送対象のコンテンツCについて全てのデータを情報利用端末2~4に配送したかどうかを調べ、まだ配送を行っていないデータがある場合にはステップ1302へ戻ってコンテンツCの配送を続行し、全データの配送を完了した場合にはコンテンツCの配送処理を終了する。

【0097】図14は本実施形態の各情報利用端末のコンテンツ利用処理の処理手順を示すフローチャートである。図14に示す様に各情報利用端末のコンテンツ取得部313は、暗号化コンテンツ K_i (C)を情報提供端末1からマルチキャストで取得し、前記取得した暗号化コンテンツ K_i (C)の暗号化で用いられた暗号鍵 K_i の識別情報 i を識別情報確認部1011により確認する。そしてコンテンツ復号化部314は、鍵保存部312によって保存されていた鍵の内、識別情報確認部1011により指定された識別情報 i の暗号鍵 K_i を用いて暗号化コンテンツ K_i (C)を復号化し、前記復号化されたコンテンツCをコンテンツ再生部315により再生する処理を行う。

【0098】図14のステップ1401で各情報利用端末のコンテンツ取得部313は、情報提供端末1からマルチキャストで暗号化コンテンツ K_i (C)を受信しているかどうかを調べ、暗号化コンテンツ K_i (C)を受信している場合にはステップ1402へ進み、前記受信した暗号化コンテンツ K_i (C)を取得して識別情報確認部1011に渡す。

【0099】ステップ1403で識別情報確認部1011は、前記取得した暗号化コンテンツ K_i (C)のヘッダー等を参照し、暗号化コンテンツ K_i (C)に付加されている識別番号 i を確認してコンテンツ復号化部314へ通知する。

【0100】ステップ1404でコンテンツ復号化部314は、識別情報確認部1011から通知されたものと同一の識別番号 i を持つ暗号鍵 K_i の読込みが未実行であるかどうかを調べ、暗号鍵 K_i の読込みが未実行である場合にはステップ1405へ進む。

【0101】ステップ1405では、鍵保存部312によってメモリ302または磁気ディスク装置303に保存されている鍵の内、識別情報確認部1011から通知されたものと同一の識別番号 i を持つ暗号鍵 K_i を読み

出す。

【0102】ステップ1406では、ステップ1402で取得した暗号化コンテンツ K_i (C)をステップ1405で読み出した暗号鍵 K_i によって復号化してコンテンツCを生成し、ステップ1407でコンテンツ再生部315は、前記復号化によって得られたコンテンツCを再生してステップ1401へ戻る。

【0103】前記の様に本実施形態では、情報提供端末1から配送されるコンテンツCの利用資格を持つ利用者の情報利用端末へユニキャストで暗号鍵 K_i (復号兼用)を配送した後、識別情報 i を付加した暗号化コンテンツ K_i (C)をマルチキャストで各情報利用端末へ配送しているので、コンテンツの利用資格を失った利用者による不正利用を防止しつつマルチキャストを利用した効率的なコンテンツの提供を行うことができる。

【0104】以上説明した様に本実施形態の情報配送システムによれば、マルチキャストで情報提供端末から各情報利用端末に配送された暗号化コンテンツを、ユニキャストで当該情報利用端末に配送された鍵によって復号化するので、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能であると言う従来の問題点を解決し、マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能である。

【0105】(実施形態3)以下に鍵提供端末の鍵を各情報利用端末から取得して鍵の更新を行った後にストリームコンテンツをマルチキャストで配送する実施形態3の情報配送システムについて説明する。

【0106】図15は本実施形態の鍵提供端末5の概略構成を示す図である。図15に示す様に本実施形態の鍵提供端末5は鍵更新広報部1511を有している。鍵更新広報部1511は、新規の鍵の取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信する処理部である。

【0107】鍵提供端末5を鍵更新広報部1511として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0108】本実施形態において、情報提供端末1は実施形態1と同様の構成であるものとし、情報提供端末1と情報利用端末2~4と鍵提供端末5は、実施形態1と同様にそれぞれインターネットに接続されており、ネットワーク上でマルチキャストとユニキャストの通信が可能であるものとする。本実施形態では、ストリームコンテンツをマルチキャストで情報利用端末2~4に配送す

る情報提供端末 1 と、そのストリームコンテンツを暗号化または復号化する為の鍵を配送する鍵提供端末 5 とが別装置であるものとして説明するが、両者を同一の装置で実現しても良い。

【0109】図 16 は本実施形態の情報利用端末 2 の概略構成を示す図である。図 16 に示す様に本実施形態の情報利用端末 2 は鍵更新情報取得部 1611 を有している。鍵更新情報取得部 1611 は、新規の鍵の取得を促す鍵更新広報を鍵提供端末 5 から取得し、新規の鍵の配送を鍵提供端末 5 に要求する処理部である。

【0110】情報利用端末 2 を鍵更新情報取得部 1611 として機能させる為のプログラムは、CD-ROM 等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体は CD-ROM 以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0111】なお情報利用端末 3 及び 4 についても情報利用端末 2 の構成と同様であるものとする。

【0112】本実施形態の情報提供端末 1 には、配送対象のストリームコンテンツが保存されているか、或いはリアルタイムでストリームコンテンツが取得されるものとし、鍵提供端末 5 から情報提供端末 1 及び情報利用端末に鍵を、また情報提供端末 1 から各情報利用端末に暗号化コンテンツを送付し、各情報利用端末で暗号化コンテンツを復号化して再生する際の例について説明する。なおこの例ではコンテンツの暗号化に利用される暗号鍵は復号鍵を兼ねており、その鍵は所定の時間間隔で更新されるものとする。なお利用資格変更に伴って鍵が更新されるものとし、公開鍵暗号方式の様に暗号鍵と復号鍵とが異なるものとしても良く、暗号鍵と復号鍵とが異なるものとした場合には、情報提供端末 1 に暗号鍵を配送し、コンテンツの利用資格を持つ利用者の情報利用端末には復号鍵の配送を行うものとする。また更新の際は鍵提供端末 5 が呼びかけ、それに応じる形で情報利用端末 2～4 が鍵の更新を行なうものとする。

【0113】図 17 は本実施形態の鍵提供端末 5 の鍵配送処理の処理手順を示すフローチャートである。図 17 に示す様に鍵提供端末 5 では、ストリームコンテンツであるコンテンツ C を暗号化または復号化する為の暗号鍵 K i を生成した後、鍵更新広報部 1511 により新規の暗号鍵 K i の取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信し、各情報利用端末からの接続を受付けてその暗号鍵 K i をユニキャストで配送する処理を行う。

【0114】図 17 のステップ 1701 で鍵提供端末 5 の鍵生成部 411 は、所定の時間が経過した場合や情報提供端末 1 の利用資格者 DB 中の利用資格が変更された

場合等の暗号鍵 K を生成する条件が成立したかどうかを調べ、暗号鍵 K を生成する条件が成立した場合にはステップ 1702 へ進む。

【0115】ステップ 1702 では、コンテンツ C を暗号化する為の暗号鍵 K を生成する。暗号鍵 K として通信時に IPsec で利用されているものを利用しても構わないものとする。

【0116】ステップ 1703 で識別情報付加部 911 は、前記生成された暗号鍵 K に識別情報 i を付加して鍵配送部 412 へ渡す。この識別情報は IPsec の SA に含まれる情報を利用しても構わないものとする。

【0117】ステップ 1704 で鍵配送部 412 は、前記生成された暗号鍵 K i をユニキャストで情報提供端末 1 へ配送する。ここで配送の際に IPsec 等を用いて通信路をセキュアな状態に保っても構わないものとする。

【0118】ステップ 1705 で鍵更新広報部 1511 は、各情報利用端末に向けて新規の暗号鍵 K i の取得を促す鍵更新広報をマルチキャストにより送信する。この広報を受け取った各情報利用端末は、暗号鍵 K i を取得する為に鍵提供端末 5 へユニキャストで接続する。

【0119】ステップ 1706 で鍵配送部 412 は、ユニキャストを用いた情報利用端末からの接続要求があるかどうかを調べ、情報利用端末からの接続要求がある場合にはステップ 1707 へ進む。

【0120】ステップ 1707 では、情報提供端末 1 の利用資格者 DB の内容を参照し、前記接続要求が、情報提供端末 1 から配送されるコンテンツ C の利用資格を持つ利用者の情報利用端末から送信されているかどうかを調べ、前記接続要求が利用資格を持つ利用者の情報利用端末から送信されている場合にはステップ 1708 へ進む。

【0121】ステップ 1708 では、前記接続要求を行った情報利用端末へユニキャストによって暗号鍵 K i を配送する。ここで配送の際に IPsec 等を用いて通信路をセキュアな状態に保っても構わないものとする。

【0122】ステップ 1709 では、前記利用資格を持つ全ての利用者の情報利用端末に暗号鍵 K i を配送したかどうかを調べ、まだ配送を行っていない情報利用端末がある場合にはステップ 1706 へ戻って他の情報利用端末からの接続要求を待ち、利用資格を持つ全ての利用者の情報利用端末への配送を完了した場合にはステップ 1710 へ進む。ここで鍵の配送の完了とは、各情報利用端末と鍵提供端末 5 がユニキャストで鍵の通信を行って正常終了した場合の他に、情報利用端末 2～4 からの応答が無く、タイムアウトした場合を含んでも構わないものとする。また鍵提供端末 5 の鍵配送に対する応答を所定時間で区切り、その区切りをもって鍵配送完了通知としても構わないものとする。

【0123】ステップ 1710 では、利用資格を持った

全ての利用者に対する暗号鍵*K_i*の配送が完了したことを示す鍵配送完了通知を鍵更新部912に伝え、ステップ1711で鍵更新部912は、配送が完了した暗号鍵*K_i*を次の暗号化処理で使用する鍵として決定し、その暗号鍵*K_i*の識別情報*i*或いは暗号鍵*K_i*そのものの情報を情報提供端末1のコンテンツ暗号化部213に通知してステップ1701へ戻る。

【0124】図18は本実施形態の情報提供端末1または各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。図18に示す様に各情報利用端末は、鍵更新情報取得部1611により新規の暗号鍵*K_i*の取得を促す鍵更新広報を鍵提供端末5から取得し、新規の暗号鍵*K_i*の配送を鍵提供端末5に要求してユニキャストで配送された暗号鍵*K_i*を取得する処理を行う。

【0125】図18のステップ1801で各情報利用端末の鍵更新情報取得部1611は、鍵提供端末5からマルチキャストで新規の暗号鍵*K_i*の取得を促す鍵更新広報を受信しているかどうかを調べ、鍵更新広報を受信している場合にはステップ1802へ進み、鍵提供端末5へユニキャストで接続して暗号鍵*K_i*の配送を要求する。

【0126】ステップ1803で鍵取得部311は、鍵提供端末5からユニキャストで暗号鍵*K_i*を受信しているかどうかを調べ、暗号鍵*K_i*を受信している場合にはその暗号鍵*K_i*を取得して鍵保存部312に渡す。

【0127】ステップ1804で鍵保存部312は、鍵提供端末5の識別情報付加部911によって付加された識別情報*i*を暗号鍵*K_i*から読み出し、ステップ1804では、ステップ1802で取得した暗号鍵*K_i*をステップ1803で読み出した識別情報*i*毎に分類してメモリ302または磁気ディスク装置303に保存する。ここで磁気ディスク装置303に保存する場合には暗号鍵*K_i*を暗号化して保存を行うものとする。

【0128】また本実施形態では、実施形態2と同様にコンテンツ配送処理を行う。すなわち、図13に示す様に情報提供端末1のコンテンツ暗号化部213は、鍵保存部212によって保存された鍵の内、鍵提供端末5の鍵更新部912により指定された識別情報*i*の暗号鍵*K_i*を用いてコンテンツ*C*を暗号化し、前記暗号化されたコンテンツである暗号化コンテンツ*K_i(C)*をコンテンツ配送部214によりマルチキャストで各情報利用端末に配送する処理を行う。

【0129】また図14に示す様に各情報利用端末のコンテンツ取得部313は、暗号化コンテンツ*K_i(C)*を情報提供端末1からマルチキャストで取得し、前記取得した暗号化コンテンツ*K_i(C)*の暗号化で用いられた暗号鍵*K_i*の識別情報*i*を識別情報確認部1011により確認する。そしてコンテンツ復号化部314は、鍵保存部312によって保存されていた鍵の内、識別情報確認部1011により指定された識別情報*i*の暗号鍵

*i*を用いて暗号化コンテンツ*K_i(C)*を復号化し、前記復号化されたコンテンツ*C*をコンテンツ再生部315により再生する処理を行う。

【0130】前記の様に本実施形態では、新規の暗号鍵*K_i*の取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信した後、情報提供端末1から配送されるコンテンツ*C*の利用資格を持つ利用者の情報利用端末へユニキャストで暗号鍵*K_i*(復号兼用)を配送した後、識別情報*i*を付加した暗号化コンテンツ*K_i(C)*をマルチキャストで各情報利用端末へ配送しているので、コンテンツの利用資格を失った利用者による不正利用を防止しつつマルチキャストを利用した効率的なコンテンツの提供を行うことができる。

【0131】以上説明した様に本実施形態の情報配送システムによれば、マルチキャストで情報提供端末から各情報利用端末に配送された暗号化コンテンツを、ユニキャストで当該情報利用端末に配送された鍵によって復号化するので、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能であると言う従来の問題点を解決し、マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能である。

【0132】(実施形態4)以下に利用者の加入及び脱退に応じてコンテンツの復号鍵の配送先を管理し、復号鍵を鍵提供端末から各情報利用端末へ配布する実施形態4の情報配送システムについて説明する。

【0133】図19は本実施形態の情報配送システムの概略構成を示す図である。本実施形態において、情報提供端末1と情報利用端末2~4と鍵提供端末5はそれぞれインターネットに接続されており、ネットワーク上でマルチキャストとユニキャストの通信が可能であるものとする。本実施形態では、ストリームコンテンツをマルチキャストで情報利用端末2~4に配送する情報提供端末1と、そのストリームコンテンツを暗号化または復号化する為の鍵を配送する鍵提供端末5とが別装置であるものとして説明するが、両者を同一の装置で実現しても良い。なお本実施形態では鍵提供端末5で鍵を生成するものとするが、情報提供端末1で鍵を生成するものとしても良い。

【0134】図20は本実施形態の鍵提供端末5の概略構成を示す図である。図20に示す様に本実施形態の鍵提供端末5は利用資格者DB2008を有している。利用資格者DB2008は、コンテンツの利用資格を持つ利用者を示す配送先リストの情報として、利用者の利用チャンネル情報や加入日時及び脱退日時を格納するデータベースである。

【0135】また鍵提供端末5は、加入要求受付部2011と、データベース部2012と、脱退要求受付部2013とを有している。

【0136】加入要求受付部2011は、前記配送先リ

ストへの加入要求を情報利用端末 2～4 から受付ける処理部である。データベース部 2012 は、前記加入要求を送信した利用者の利用チャンネルと利用者の利用資格が発生する日時を示す加入日時とを利用資格者 DB 2008 に格納する処理部である。脱退要求受付部 2013 は、前記配送先リストからの脱退要求を情報利用端末 2～4 から受付ける処理部である。

【0137】鍵提供端末 5 を加入要求受付部 2011、データベース部 2012 及び脱退要求受付部 2013 として機能させる為のプログラムは、CD-ROM 等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体は CD-ROM 以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0138】本実施形態において、鍵提供端末 5 のその他の構成は実施形態 2 と同様であるものとし、情報提供端末 1 は利用資格者 DB 2008 が鍵提供端末 5 にあることを除いて実施形態 1 と同様の構成であるものとする。

【0139】図 21 は本実施形態の情報利用端末 2 の概略構成を示す図である。図 21 に示す様に本実施形態の情報利用端末 2 は、加入要求部 2111 と、脱退要求部 2112 とを有している。

【0140】加入要求部 2111 は、前記配送先リストへの加入要求を鍵提供端末 5 に送信する処理部である。脱退要求部 2112 は、前記配送先リストからの脱退要求を鍵提供端末 5 に送信する処理部である。

【0141】情報利用端末 2 を加入要求部 2111 及び脱退要求部 2112 として機能させる為のプログラムは、CD-ROM 等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体は CD-ROM 以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0142】本実施形態において、情報利用端末 2 のその他の構成は実施形態 2 と同様であるものとし、情報利用端末 3 及び 4 についても情報利用端末 2 の構成と同様であるものとする。

【0143】本実施形態の情報提供端末 1 には、配送対象のストリームコンテンツが保存されているか、或いはリアルタイムでストリームコンテンツが取得されるものとし、鍵提供端末 5 から情報提供端末 1 及び各情報利用端末に鍵を、また情報提供端末 1 から各情報利用端末に暗号化コンテンツを送付し、各情報利用端末で暗号化コ

ンテンツを復号化して再生する際の例について説明する。なおこの例ではコンテンツの暗号化に利用される暗号鍵は復号鍵を兼ねており、その鍵は所定の時間間隔で更新されるものとする。なお利用資格変更に伴って鍵が更新されるものとしたり、公開鍵暗号方式の様に暗号鍵と復号鍵とが異なるものとしても良く、暗号鍵と復号鍵とが異なるものとした場合には、情報提供端末 1 に暗号鍵を配送し、コンテンツの利用資格を持つ利用者の情報利用端末には復号鍵の配送を行うものとする。

10 【0144】図 22 は本実施形態の加入要求処理の処理手順を示すフローチャートである。図 22 に示す様に各情報利用端末の加入要求部 2111 は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を鍵提供端末 5 に送信する処理を行う。

【0145】ステップ 2201 で各情報利用端末の加入要求部 2111 は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入指示の利用者からの入力を受付けているかどうかを調べ、前記配送先リストへの加入指示を受付けている場合にはステップ 2202 へ進む。

20 【0146】ステップ 2202 では、当該情報利用端末を一意に指定できる情報として、情報利用端末の識別子、IP アドレス、サービス加入時のユーザ情報または端末情報等を磁気ディスク装置 303 から読み出す。

【0147】ステップ 2203 では、利用者が加入したいチャンネル情報として、コンテンツの名称、コンテンツ識別情報、マルチキャストアドレス等の情報と、当該コンテンツの利用を開始したい日時を示す加入日時の入力を受付ける。ここで当該コンテンツの利用可能な期間を示す加入期間や、当該コンテンツの利用を終了したい日時を示す脱退日時の入力を受付けても良い。また加入日時を省略しても構わないものとし、省略可能とする場合は省略時の加入日時は「即時」であるとする等予め規則を決めておくものとする。

30 【0148】ステップ 2204 では、前記読み出した当該情報利用端末を一意に指定できる情報及び前記受付けたチャンネル情報と共に、前記配送先リストへの加入要求を鍵提供端末 5 に送信する。

40 【0149】図 23 は本実施形態の加入要求受付処理の処理手順を示すフローチャートである。図 23 に示す様に鍵提供端末 5 の加入要求受付部 2011 は、前記配送先リストへの加入要求を情報利用端末 2～4 から受付ける処理を行う。またデータベース部 2012 は、前記加入要求を送信した利用者の利用チャンネルと利用者の利用資格が発生する日時を示す加入日時とを利用資格者 DB 2008 に格納する処理を行う。

50 【0150】ステップ 2301 で鍵提供端末 5 の加入要求受付部 2011 は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求と情報利用端末を一意に指定できる情報及びチャンネル情報を情報利用端末 2

へ4から受信しているかどうかを調べ、前記配送先リストへの加入要求を受信している場合にはステップ2302へ進む。

【0151】ステップ2302でデータベース部2012は、前記加入要求と共に送信された、情報利用端末の識別子、IPアドレス、サービス加入時のユーザ情報または端末情報等の情報利用端末を一意に指定できる情報や、コンテンツの名称、コンテンツ識別情報、マルチキャストアドレス等のチャンネル情報、当該コンテンツの利用を開始したい日時を示す加入日時を利用資格者DB2008に格納する。ここで当該コンテンツの利用可能な期間を示す加入期間や、当該コンテンツの利用を終了したい日時を示す脱退日時も送信されている場合には、脱退日時の格納も行う。また加入日時が省略されている場合には、予め決められている規則に従って加入日時を「即時」等に設定する。

【0152】図24は本実施形態の脱退要求処理の処理手順を示すフローチャートである。図24に示す様に各情報利用端末の脱退要求部2112は、前記配送先リストからの脱退要求を鍵提供端末5に送信する処理を行う。なお加入要求時に加入期間や脱退日時の入力を行っている場合にはこの脱退要求処理を省略することができる。

【0153】ステップ2401で各情報利用端末の脱退要求部2112は、コンテンツの利用資格を持つ利用者を示す配送先リストからの脱退指示の利用者からの入力を受付けているかどうかを調べ、前記配送先リストからの脱退指示を受付けている場合にはステップ2402へ進む。

【0154】ステップ2402では、当該情報利用端末を一意に指定できる情報として、情報利用端末の識別子、IPアドレス、サービス脱退時のユーザ情報または端末情報等を磁気ディスク装置303から読み出す。

【0155】ステップ2403では、利用者が脱退したいチャンネル情報として、コンテンツの名称、コンテンツ識別情報、マルチキャストアドレス等の情報と、当該コンテンツの利用を終了したい日時を示す脱退日時の入力を受付ける。ここで脱退日時を省略しても構わないものとし、省略可能とする場合は省略時の脱退日時は「即時」であるとする等予め規則を決めておくものとする。

【0156】ステップ2404では、前記読み出した当該情報利用端末を一意に指定できる情報及び前記受付けたチャンネル情報と共に、前記配送先リストからの脱退要求を鍵提供端末5に送信する。

【0157】図25は本実施形態の脱退要求受付処理の処理手順を示すフローチャートである。図25に示す様に鍵提供端末5の脱退要求受付部2013は、前記配送先リストからの脱退要求を情報利用端末2～4から受付ける処理を行う。

【0158】ステップ2501で鍵提供端末5の脱退要

求受付部2013は、コンテンツの利用資格を持つ利用者を示す配送先リストからの脱退要求と情報利用端末を一意に指定できる情報及びチャンネル情報を情報利用端末2～4から受信しているかどうかを調べ、前記配送先リストへの脱退要求を受信している場合にはステップ2502へ進む。

【0159】ステップ2502でデータベース部2012は、前記脱退要求と共に送信された情報利用端末を一意に指定できる情報及びチャンネル情報に該当するレコードを利用資格者DB2008から検索し、前記チャンネル情報中の脱退日時の情報を当該レコードに格納する。また脱退日時が省略されている場合には、予め決められている規則に従って脱退日時を「即時」等に設定する。

【0160】図26は本実施形態の鍵提供端末5の鍵配送処理の処理手順を示すフローチャートである。図26に示す様に鍵提供端末5の鍵生成部411は、ストリームコンテンツであるコンテンツCを暗号化または復号化する為の暗号鍵Kを生成し、前記生成された暗号鍵Kにその鍵を識別する為の識別情報iを識別情報付加部911により付加する。また鍵配送部412により情報提供端末1及び各情報利用端末にその暗号鍵Kiをユニキャストで配送した後、次の暗号化処理で使用する鍵の識別情報iを鍵更新部912により情報提供端末1に指定する処理を行う。

【0161】図26のステップ2601で鍵提供端末5の鍵生成部411は、所定の時間が経過した場合や情報提供端末1の利用資格者DB2008中の利用資格が変更された場合等の暗号鍵Kを生成する条件が成立したかどうかを調べ、暗号鍵Kを生成する条件が成立した場合にはステップ2602へ進む。

【0162】ステップ2602では、コンテンツCを暗号化する為の暗号鍵Kを生成する。暗号鍵Kとして通信時にIPsecで利用されているものを利用しても構わないものとする。

【0163】ステップ2603で識別情報付加部911は、前記生成された暗号鍵Kに識別情報iを付加して鍵配送部412へ渡す。この識別情報はIPsecのSAに含まれる情報を利用して構わないものとする。

【0164】ステップ2604で鍵配送部412は、前記生成された暗号鍵Kiをユニキャストで情報提供端末1へ配送する。ここで配送の際にIPsec等を用いて通信路をセキュアな状態に保っても構わないものとする。

【0165】ステップ2605で鍵配送部412は、情報提供端末1の利用資格者DB2008の内容を参照し、情報提供端末1から配送されるコンテンツCの名称がそのチャンネル情報に含まれているレコードの加入日時及び脱退日時を読み出す。

【0166】ステップ2606では、現在の日時と利用資格者DB2008から前記読み出した加入日時とを比

較し、それらの差が所定の時間以内であるかまたは現在の日時が前記加入日時を経過している場合にはステップ 2607 へ進む。

【0167】ステップ 2607 では、現在の日時と利用資格者 DB 2008 から前記読み出した脱退日時とを比較し、現在の日時が前記脱退日時を経過しておらず、配送対象の鍵が脱退日時以前に配送されるコンテンツの鍵である場合にはステップ 2608 へ進む。

【0168】ステップ 2608 では、前記レコードから、その情報利用端末の IP アドレスを読み出し、その IP アドレスを宛先としたユニキャストによって暗号鍵 K_i を配送する。ここで配送の際に IPsec 等を用いて通信路をセキュアな状態に保っても構わないものとする。

【0169】ステップ 2609 では、前記利用資格を持つ全ての利用者の情報利用端末に暗号鍵 K_i を配送したかどうかを調べ、まだ配送を行っていない情報利用端末がある場合にはステップ 2605 へ戻って暗号鍵 K_i の配送を続行し、利用資格を持つ全ての利用者の情報利用端末への配送を完了した場合にはステップ 2610 へ進む。ここで鍵の配送の完了とは、各情報利用端末と鍵提供端末 5 がユニキャストで鍵の通信を行って正常終了した場合の他に、情報利用端末 2～4 からの応答が無く、タイムアウトした場合を含んでいても構わないものとする。

【0170】ステップ 2610 では、利用資格を持った全ての利用者に対する暗号鍵 K_i の配送が完了したことを示す鍵配送完了通知を鍵更新部 912 に伝え、ステップ 2611 で鍵更新部 912 は、配送が完了した暗号鍵 K_i を次の暗号化処理で使用する鍵として決定し、その暗号鍵 K_i の識別情報 i 或いは暗号鍵 K_i そのものの情報を情報提供端末 1 のコンテンツ暗号化部 213 に通知してステップ 2601 へ戻る。

【0171】次に本実施形態の情報利用端末 2～4 では、実施形態 2 と同様にして暗号鍵 K_i を取得する。すなわち図 12 に示す様に情報利用端末 2～4 の鍵取得部 311 は、鍵提供端末 5 からユニキャストで暗号鍵 K_i を受信して鍵保存部 312 に渡し、鍵保存部 312 は、鍵提供端末 5 の識別情報付加部 911 によって付加された識別情報 i を暗号鍵 K_i から読み出し、暗号鍵 K_i を識別情報 i 毎に分類してメモリ 302 または磁気ディスク装置 303 に保存する。ここで各情報利用端末が暗号鍵 K_i を磁気ディスク装置 303 に保存する場合には暗号鍵 K_i を暗号化して保存を行うものとし、利用し終わった鍵は消去或いは破壊される場合もあるものとする。

【0172】また本実施形態では、実施形態 2 と同様にしてコンテンツ配送処理を行う。すなわち、図 13 に示す様に情報提供端末 1 のコンテンツ暗号化部 213 は、鍵保存部 212 によって保存された鍵の内、鍵提供端末 5 の鍵更新部 912 により指定された識別情報 i の暗号

鍵 K_i を用いてコンテンツ C を暗号化し、前記暗号化されたコンテンツである暗号化コンテンツ K_i (C) をコンテンツ配送部 214 によりマルチキャストで各情報利用端末に配送する処理を行う。

【0173】また図 14 に示す様に各情報利用端末のコンテンツ取得部 313 は、暗号化コンテンツ K_i (C) を情報提供端末 1 からマルチキャストで取得し、前記取得した暗号化コンテンツ K_i (C) の暗号化で用いられた暗号鍵 K_i の識別情報 i を識別情報確認部 1011 により確認する。そしてコンテンツ復号化部 314 は、鍵保存部 312 によって保存されていた鍵の内、識別情報確認部 1011 により指定された識別情報 i の暗号鍵 K_i を用いて暗号化コンテンツ K_i (C) を復号化し、前記復号化されたコンテンツ C をコンテンツ再生部 315 により再生する処理を行う。

【0174】前記の様に本実施形態の鍵提供端末 5 は、利用資格者 DB 2008 のデータを基に鍵を配送するため、脱退日時が経過したもの或いは次配送の鍵が脱退日時以降のコンテンツに該当する鍵である場合に情報利用端末への鍵の配送を取り止めることができる。

【0175】以上説明した様に本実施形態の情報配送システムによれば、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求の受付が行われた利用者の情報利用端末に対して復号鍵を配送するので、利用者がコンテンツの利用資格を失っても復号する手段を保持し続けることが可能であると言う問題点を解決し、マルチキャストで配送するストリームコンテンツに対して、利用者の入れ替わりに対応できる利用制御を行うことが可能である。

【0176】（実施形態 5）以下に利用者の加入及び脱退に応じてコンテンツの復号鍵の配送先を管理し、鍵更新広報により鍵提供端末の復号鍵を各情報利用端末から取得する実施形態 5 の情報配送システムについて説明する。

【0177】図 27 は本実施形態の鍵提供端末 5 の概略構成を示す図である。図 27 に示す様に本実施形態の鍵提供端末 5 は、加入要求応答部 2711 と、脱退要求応答部 2712 とを有している。

【0178】加入要求応答部 2711 は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求が受け付けられたことを示す加入要求応答を、当該加入要求を送信した情報利用端末へ通知する処理部である。脱退要求応答部 2712 は、前記配送先リストからの脱退要求が受け付けられたことを示す脱退要求応答を、当該脱退要求を送信した情報利用端末へ通知する処理部である。

【0179】鍵提供端末 5 を加入要求応答部 2711 及び脱退要求応答部 2712 として機能させる為のプログラムは、CD-ROM 等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行され

るものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0180】本実施形態において、情報提供端末1と情報利用端末2～4と鍵提供端末5は、実施形態1と同様にそれぞれインターネットに接続されており、ネットワーク上でマルチキャストとユニキャストの通信が可能であるものとする。本実施形態では、ストリームコンテンツをマルチキャストで情報利用端末2～4に配送する情報提供端末1と、そのストリームコンテンツを暗号化または復号化する為の鍵を配送する鍵提供端末5とが別装置であるものとして説明するが、両者を同一の装置で実現しても良い。また本実施形態では鍵提供端末5で鍵を生成するものとするが、情報提供端末1で鍵を生成するものとしても良い。

【0181】なお本実施形態において、鍵提供端末5のその他の構成は実施形態3と同様であるものとし、情報提供端末1は利用資格者DB2008が鍵提供端末5にあることを除いて実施形態1と同様の構成であるものとする。

【0182】図28は本実施形態の情報利用端末2の概略構成を示す図である。図28に示す様に本実施形態の情報利用端末2は、加入要求応答受付部2811と、脱退要求応答受付部2812とを有している。

【0183】加入要求応答受付部2811は、前記配送先リストへの加入要求が受け付けられたことを示す加入要求応答を鍵提供端末5から受信する処理部である。脱退要求応答受付部2812は、前記配送先リストからの脱退要求が受け付けられたことを示す脱退要求応答を鍵提供端末5から受信する処理部である。

【0184】情報利用端末2を加入要求応答受付部2811及び脱退要求応答受付部2812として機能させる為のプログラムは、CD-ROM等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はCD-ROM以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0185】本実施形態において、情報利用端末2のその他の構成は実施形態3と同様であるものとし、情報利用端末3及び4についても情報利用端末2の構成と同様であるものとする。

【0186】本実施形態の情報提供端末1には、配送対象のストリームコンテンツが保存されているか、或いはリアルタイムでストリームコンテンツが取得されるもの

とし、鍵提供端末5から情報提供端末1及び情報利用端末に鍵を、また情報提供端末1から各情報利用端末に暗号化コンテンツを送付し、各情報利用端末で暗号化コンテンツを復号化して再生する際の例について説明する。なおこの例ではコンテンツの暗号化に利用される暗号鍵は復号鍵を兼ねており、その鍵は所定の時間間隔で更新されるものとする。なお利用資格変更に伴って鍵が更新されるものとし、公開鍵暗号方式の様に暗号鍵と復号鍵とが異なるものとしても良く、暗号鍵と復号鍵とが異なるものとした場合には、情報提供端末1に暗号鍵を配送し、コンテンツの利用資格を持つ利用者の情報利用端末には復号鍵の配送を行うものとする。また更新の際は鍵提供端末5が呼びかけ、それに応じる形で情報利用端末2～4が鍵の更新を行なうものとする。

【0187】図29は本実施形態の加入要求処理の処理手順を示すフローチャートである。図29に示す様に各情報利用端末の加入要求部2111は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求を鍵提供端末5に送信する処理を行い、加入要求応答受付部2811は、前記配送先リストへの加入要求が受け付けられたことを示す加入要求応答を鍵提供端末5から受信する処理を行う。

【0188】ステップ2901で各情報利用端末の加入要求部2111は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入指示の利用者からの入力を受け付けているかどうかを調べ、前記配送先リストへの加入指示を受け付けている場合にはステップ2902へ進む。

【0189】ステップ2902では、当該情報利用端末を一意に指定できる情報として、情報利用端末の識別子、IPアドレス、サービス加入時のユーザ情報または端末情報等を磁気ディスク装置303から読み出す。

【0190】ステップ2903では、利用者が加入したいチャンネル情報として、コンテンツの名称、コンテンツ識別情報、マルチキャストアドレス等の情報と、当該コンテンツの利用を開始したい日時を示す加入日時の入力を受け付ける。ここで当該コンテンツの利用可能な期間を示す加入期間や、当該コンテンツの利用を終了したい日時を示す脱退日時の入力を受け付けても良い。また加入日時を省略しても構わないものとし、省略可能とする場合は省略時の加入日時は「即時」とであるとする等予め規則を決めておくものとする。

【0191】ステップ2904では、前記読み出した当該情報利用端末を一意に指定できる情報及び前記受け付けたチャンネル情報と共に、前記配送先リストへの加入要求を鍵提供端末5に送信する。

【0192】ステップ2905で加入要求応答受付部2811は、前記配送先リストからの加入要求が受け付けられたことを示す加入要求応答を鍵提供端末5から受信しているかどうかを調べ、前記加入要求応答を受信してい

る場合にはステップ 2906 へ進む。ステップ 2906 では、前記受信した加入要求応答の内容を出力装置 305 へ表示して加入要求の結果を利用者へ知らせる。

【0193】図 30 は本実施形態の加入要求受付処理の処理手順を示すフローチャートである。図 30 に示す様に鍵提供端末 5 の加入要求受付部 2011 は、前記配送先リストへの加入要求を情報利用端末 2~4 から受け付ける処理を行い、加入要求応答部 2711 は、前記配送先リストへの加入要求が受け付けられたことを示す加入要求応答を、当該加入要求を送信した情報利用端末へ通知する処理を行う。

【0194】ステップ 3001 で鍵提供端末 5 の加入要求受付部 2011 は、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求と情報利用端末を一意に指定できる情報及びチャンネル情報を情報利用端末 2~4 から受信しているかどうかを調べ、前記配送先リストへの加入要求を受信している場合にはステップ 3002 へ進む。

【0195】ステップ 3002 でデータベース部 2012 は、前記加入要求と共に送信された、情報利用端末の識別子、IP アドレス、サービス加入時のユーザ情報または端末情報等の情報利用端末を一意に指定できる情報や、コンテンツの名称、コンテンツ識別情報、マルチキャストアドレス等のチャンネル情報、当該コンテンツの利用を開始したい日時を示す加入日時を利用資格者 DB 2008 に格納する。ここで当該コンテンツの利用可能な期間を示す加入期間や、当該コンテンツの利用を終了したい日時を示す脱退日時も送信されている場合には、脱退日時の格納も行う。また加入日時が省略されている場合には、予め決められている規則に従って加入日時を「即時」等に設定する。

【0196】ステップ 3003 で加入要求応答部 2711 は、前記配送先リストへの加入要求が受け付けられたことを示す加入要求応答を、当該加入要求を送信した情報利用端末へ通知する処理を行う。

【0197】図 31 は本実施形態の脱退要求処理の処理手順を示すフローチャートである。図 31 に示す様に各情報利用端末の脱退要求部 2112 は、前記配送先リストからの脱退要求を鍵提供端末 5 に送信する処理を行い、脱退要求応答受付部 2812 は、前記配送先リストからの脱退要求が受け付けられたことを示す脱退要求応答を鍵提供端末 5 から受信する処理を行う。なお加入要求時に加入期間や脱退日時の入力を行っている場合にはこの脱退要求処理を省略することができる。

【0198】ステップ 3101 で各情報利用端末の脱退要求部 2112 は、コンテンツの利用資格を持つ利用者を示す配送先リストからの脱退指示の利用者からの入力を受け付けているかどうかを調べ、前記配送先リストからの脱退指示を受け付けている場合にはステップ 3102 へ進む。

【0199】ステップ 3102 では、当該情報利用端末を一意に指定できる情報として、情報利用端末の識別子、IP アドレス、サービス脱退時のユーザ情報または端末情報等を磁気ディスク装置 303 から読み出す。

【0200】ステップ 3103 では、利用者が脱退したいチャンネル情報として、コンテンツの名称、コンテンツ識別情報、マルチキャストアドレス等の情報と、当該コンテンツの利用を終了したい日時を示す脱退日時の入力を受け付ける。ここで脱退日時を省略しても構わないものとし、省略可能とする場合は省略時の脱退日時は「即時」であるとする等予め規則を決めておくものとする。

【0201】ステップ 3104 では、前記読み出した当該情報利用端末を一意に指定できる情報及び前記受け付けたチャンネル情報と共に、前記配送先リストからの脱退要求を鍵提供端末 5 に送信する。

【0202】ステップ 3105 で脱退要求応答受付部 2812 は、前記配送先リストからの脱退要求が受け付けられたことを示す脱退要求応答を鍵提供端末 5 から受信しているかどうかを調べ、前記脱退要求応答を受信している場合にはステップ 3106 へ進む。ステップ 3106 では、前記受信した脱退要求応答の内容を出力装置 305 へ表示して脱退要求の結果を利用者へ知らせる。

【0203】図 32 は本実施形態の脱退要求受付処理の処理手順を示すフローチャートである。図 32 に示す様に鍵提供端末 5 の脱退要求受付部 2013 は、前記配送先リストからの脱退要求を情報利用端末 2~4 から受け付ける処理を行い、脱退要求応答部 2712 は、前記配送先リストからの脱退要求が受け付けられたことを示す脱退要求応答を、当該脱退要求を送信した情報利用端末へ通知する処理を行う。

【0204】ステップ 3201 で鍵提供端末 5 の脱退要求受付部 2013 は、コンテンツの利用資格を持つ利用者を示す配送先リストからの脱退要求と情報利用端末を一意に指定できる情報及びチャンネル情報を情報利用端末 2~4 から受信しているかどうかを調べ、前記配送先リストへの脱退要求を受信している場合にはステップ 3202 へ進む。

【0205】ステップ 3202 でデータベース部 2012 は、前記脱退要求と共に送信された情報利用端末を一意に指定できる情報及びチャンネル情報に該当するレコードを利用資格者 DB 2008 から検索し、前記チャンネル情報中の脱退日時の情報を当該レコードに格納する。また脱退日時が省略されている場合には、予め決められている規則に従って脱退日時を「即時」等に設定する。

【0206】ステップ 3203 で脱退要求応答部 2712 は、前記配送先リストからの脱退要求が受け付けられたことを示す脱退要求応答を、当該脱退要求を送信した情報利用端末へ通知する処理を行う。

【0207】図 33 は本実施形態の鍵提供端末 5 の鍵配送処理の処理手順を示すフローチャートである。図 33

に示す様に鍵提供端末 5 では、ストリームコンテンツであるコンテンツ C を暗号化または復号化する為の暗号鍵 K i を生成した後、鍵更新広報部 1511 により新規の暗号鍵 K i の取得を促す鍵更新広報をマルチキャストで各情報利用端末に送信し、各情報利用端末からの接続を受付けてその暗号鍵 K i をユニキャストで配送する処理を行う。

【0208】図 33 のステップ 3301 で鍵提供端末 5 の鍵生成部 411 は、所定の時間が経過した場合や情報提供端末 1 の利用資格者 DB2008 中の利用資格が変更された場合等の暗号鍵 K を生成する条件が成立したかどうかを調べ、暗号鍵 K を生成する条件が成立した場合にはステップ 3302 へ進む。

【0209】ステップ 3302 では、コンテンツ C を暗号化する為の暗号鍵 K を生成する。暗号鍵 K として通信時に IPsec で利用されているものを利用して構わないものとする。

【0210】ステップ 3303 で識別情報付加部 911 は、前記生成された暗号鍵 K に識別情報 i を付加して鍵配送部 412 へ渡す。この識別情報は IPsec の SA に含まれる情報を利用して構わないものとする。

【0211】ステップ 3304 で鍵配送部 412 は、前記生成された暗号鍵 K i をユニキャストで情報提供端末 1 へ配送する。ここで配送の際に IPsec 等を用いて通信路をセキュアな状態に保っても構わないものとする。

【0212】ステップ 3305 で鍵更新広報部 1511 は、各情報利用端末に向けて新規の暗号鍵 K i の取得を促す鍵更新広報をマルチキャストにより送信する。ここで利用資格者 DB2008 を検索して鍵の配送の対象となる利用者を特定し、その利用者の情報利用端末に対してユニキャストで鍵更新広報を通知しても構わないものとする。この広報を受け取った各情報利用端末は、暗号鍵 K i を取得する為に鍵提供端末 5 へユニキャストで接続する。

【0213】ステップ 3306 で鍵配送部 412 は、ユニキャストを用いた情報利用端末からの接続要求があるかどうかを調べ、情報利用端末からの接続要求がある場合にはステップ 3307 へ進む。

【0214】ステップ 3307 では、情報提供端末 1 の利用資格者 DB2008 の内容を参照し、前記接続要求を送信した利用者のレコードの加入日時及び脱退日時を読み出す。

【0215】ステップ 3308 では、現在の日時と利用資格者 DB2008 から前記読み出した加入日時とを比較し、それらの差が所定の時間以内であるかまたは現在の日時が前記加入日時を経過している場合にはステップ 3309 へ進む。

【0216】ステップ 3309 では、現在の日時と利用資格者 DB2008 から前記読み出した脱退日時とを比

較し、現在の日時が前記脱退日時を経過しておらず、配送対象の鍵が脱退日時以前に配送されるコンテンツの鍵である場合にはステップ 3310 へ進む。

【0217】ステップ 3310 では、前記レコードから前記接続要求を行った情報利用端末の IP アドレスを読み出し、その IP アドレスを宛先としたユニキャストによって暗号鍵 K i を配送する。ここで配送の際に IPsec 等を用いて通信路をセキュアな状態に保っても構わないものとする。

10 【0218】ステップ 3311 では、前記利用資格を持つ全ての利用者の情報利用端末に暗号鍵 K i を配送したかどうかを調べ、まだ配送を行っていない情報利用端末がある場合にはステップ 3306 へ戻って他の情報利用端末からの接続要求を待ち、利用資格を持つ全ての利用者の情報利用端末への配送を完了した場合にはステップ 3312 へ進む。ここで鍵の配送の完了とは、各情報利用端末と鍵提供端末 5 がユニキャストで鍵の通信を行って正常終了した場合の他に、情報利用端末 2~4 からの応答が無く、タイムアウトした場合を含んでも構わないものとする。また鍵提供端末 5 の鍵配送に対する応答を所定時間で区切り、その区切りをもって鍵配送完了通知としても構わないものとする。

20 【0219】ステップ 3312 では、利用資格を持った全ての利用者に対する暗号鍵 K i の配送が完了したことを示す鍵配送完了通知を鍵更新部 912 に伝え、ステップ 3313 で鍵更新部 912 は、配送が完了した暗号鍵 K i を次の暗号化処理で使用する鍵として決定し、その暗号鍵 K i の識別情報 i 或いは暗号鍵 K i そのものの情報を情報提供端末 1 のコンテンツ暗号化部 213 に通知してステップ 3301 へ戻る。

30 【0220】次に本実施形態の情報利用端末 2~4 では、実施形態 3 と同様にして暗号鍵 K i を取得する。すなわち図 18 に示す様に各情報利用端末の鍵更新情報取得部 1611 は、鍵提供端末 5 からマルチキャストで新規の暗号鍵 K i の取得を促す鍵更新広報を受信して鍵提供端末 5 へユニキャストで接続し、鍵提供端末 5 からユニキャストで暗号鍵 K i を受信して鍵保存部 312 に渡す。そして鍵保存部 312 は、鍵提供端末 5 の識別情報付加部 911 によって付加された識別情報 i 毎に暗号鍵 K i を分類してメモリ 302 または磁気ディスク装置 303 に保存する。ここで磁気ディスク装置 303 に保存する場合には暗号鍵 K i を暗号化して保存を行うものとし、利用し終わった鍵は消去或いは破壊される場合もあるものとする。

50 【0221】また本実施形態では、実施形態 2 と同様にしてコンテンツ配送処理を行う。すなわち、図 13 に示す様に情報提供端末 1 のコンテンツ暗号化部 213 は、鍵保存部 212 によって保存された鍵の内、鍵提供端末 5 の鍵更新部 912 により指定された識別情報 i の暗号鍵 K i を用いてコンテンツ C を暗号化し、前記暗号化さ

れたコンテンツである暗号化コンテンツ $K_i(C)$ をコンテンツ配送部 214 によりマルチキャストで各情報利用端末に配送する処理を行う。

【0222】また図 14 に示す様に各情報利用端末のコンテンツ取得部 313 は、暗号化コンテンツ $K_i(C)$ を情報提供端末 1 からマルチキャストで取得し、前記取得した暗号化コンテンツ $K_i(C)$ の暗号化で用いられた暗号鍵 K_i の識別情報 i を識別情報確認部 1011 により確認する。そしてコンテンツ復号化部 314 は、鍵保存部 312 によって保存されていた鍵の内、識別情報確認部 1011 により指定された識別情報 i の暗号鍵 K_i を用いて暗号化コンテンツ $K_i(C)$ を復号化し、前記復号化されたコンテンツ C をコンテンツ再生部 315 により再生する処理を行う。

【0223】前記の様に本実施形態の鍵提供端末 5 は、利用資格者 DB 2008 のデータを基に鍵を配送するため、鍵提供端末 5 からの鍵更新広報に対して情報利用端末から鍵の取得要求が行われた場合でも、脱退日時が経過したり、或いは次配送の鍵が脱退日時以降のコンテンツの鍵である場合に当該情報利用端末への鍵の配送を取り止めることができる。

【0224】以上説明した様に本実施形態の情報配送システムによれば、コンテンツの利用資格を持つ利用者を示す配送先リストへの加入要求の受付が行われた利用者の情報利用端末に対して復号鍵を配送するので、利用者がコンテンツの利用資格を失っても復号する手段を保持し続けることが可能であると言う問題点を解決し、マルチキャストで配送するストリームコンテンツに対して、利用者の入れ替わりに対応できる利用制御を行うことが可能である。

【0225】

【発明の効果】本発明によればマルチキャストで情報提供端末から各情報利用端末に配送された暗号化コンテンツを、ユニキャストで当該情報利用端末に配送された鍵によって復号化するので、利用者がコンテンツの利用資格を失っても復号化する手段を保持し続けることが可能であると言う従来の問題点を解決し、マルチキャストで配送されるコンテンツに対して、利用者の入れ替わりに対応した利用制御を行うことが可能である。

【図面の簡単な説明】

【図 1】実施形態 1 の情報配送システムの概略構成を示す図である。

【図 2】実施形態 1 の情報提供端末 1 の概略構成を示す図である。

【図 3】実施形態 1 の情報利用端末 2 の概略構成を示す図である。

【図 4】実施形態 1 の鍵提供端末 5 の概略構成を示す図である。

【図 5】実施形態 1 の鍵提供端末 5 の鍵配送処理の処理手順を示すフローチャートである。

【図 6】実施形態 1 の情報提供端末 1 または各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。

【図 7】実施形態 1 の情報提供端末 1 のコンテンツ配送処理の処理手順を示すフローチャートである。

【図 8】実施形態 1 の各情報利用端末のコンテンツ利用処理の処理手順を示すフローチャートである。

【図 9】実施形態 2 の鍵提供端末 5 の概略構成を示す図である。

10 【図 10】実施形態 2 の情報利用端末 2 の概略構成を示す図である。

【図 11】実施形態 2 の鍵提供端末 5 の鍵配送処理の処理手順を示すフローチャートである。

【図 12】実施形態 2 の情報提供端末 1 または各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。

【図 13】実施形態 2 の情報提供端末 1 のコンテンツ配送処理の処理手順を示すフローチャートである。

20 【図 14】実施形態 2 の各情報利用端末のコンテンツ利用処理の処理手順を示すフローチャートである。

【図 15】実施形態 3 の鍵提供端末 5 の概略構成を示す図である。

【図 16】実施形態 3 の情報利用端末 2 の概略構成を示す図である。

【図 17】実施形態 3 の鍵提供端末 5 の鍵配送処理の処理手順を示すフローチャートである。

【図 18】実施形態 3 の情報提供端末 1 または各情報利用端末の鍵取得処理の処理手順を示すフローチャートである。

30 【図 19】実施形態 4 の情報配送システムの概略構成を示す図である。

【図 20】実施形態 4 の鍵提供端末 5 の概略構成を示す図である。

【図 21】実施形態 4 の情報利用端末 2 の概略構成を示す図である。

【図 22】実施形態 4 の加入要求処理の処理手順を示すフローチャートである。

【図 23】実施形態 4 の加入要求受付処理の処理手順を示すフローチャートである。

40 【図 24】実施形態 4 の脱退要求処理の処理手順を示すフローチャートである。

【図 25】実施形態 4 の脱退要求受付処理の処理手順を示すフローチャートである。

【図 26】実施形態 4 の鍵提供端末 5 の鍵配送処理の処理手順を示すフローチャートである。

【図 27】実施形態 5 の鍵提供端末 5 の概略構成を示す図である。

【図 28】実施形態 5 の情報利用端末 2 の概略構成を示す図である。

50 【図 29】実施形態 5 の加入要求処理の処理手順を示す

フローチャートである。

【図 30】実施形態 5 の加入要求受付処理の処理手順を示すフローチャートである。

【図 31】実施形態 5 の脱退要求処理の処理手順を示すフローチャートである。

【図 32】実施形態 5 の脱退要求受付処理の処理手順を示すフローチャートである。

【図 33】実施形態 5 の鍵提供端末 5 の鍵配送処理の処理手順を示すフローチャートである。

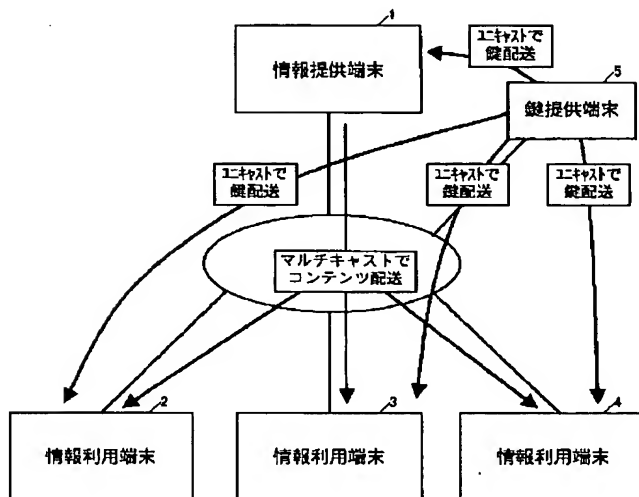
【符号の説明】

1…情報提供端末、2～4…情報利用端末、5…鍵提供端末、201…CPU、202…メモリ、203…磁気ディスク装置、204…入力装置、205…出力装置、206…CD-ROM装置、207…通信装置、211…鍵取得部、212…鍵保存部、213…コンテンツ暗号化部、214…コンテンツ配送部、301…CPU、

302…メモリ、303…磁気ディスク装置、304…入力装置、305…出力装置、306…CD-ROM装置、307…通信装置、311…鍵取得部、312…鍵保存部、313…コンテンツ取得部、314…コンテンツ復号化部、315…コンテンツ再生部、401…CPU、402…メモリ、403…磁気ディスク装置、404…入力装置、405…出力装置、406…CD-ROM装置、407…通信装置、411…鍵生成部、412…鍵配送部、911…識別情報付加部、912…鍵更新部、1011…識別情報確認部、1511…鍵更新広報部、1611…鍵更新情報取得部、2008…利用資格者DB、2011…加入要求受付部、2012…データベース部、2013…脱退要求受付部、2111…加入要求部、2112…脱退要求部、2711…加入要求応答部、2712…脱退要求応答部、2811…加入要求応答受付部、2812…脱退要求応答受付部。

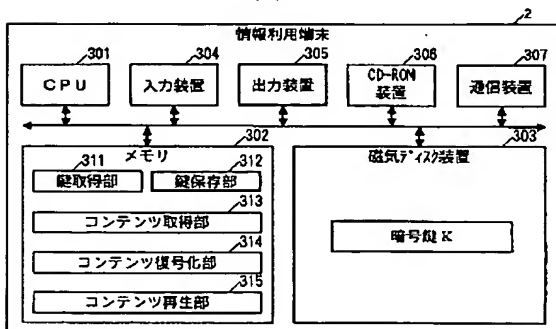
【図 1】

図 1



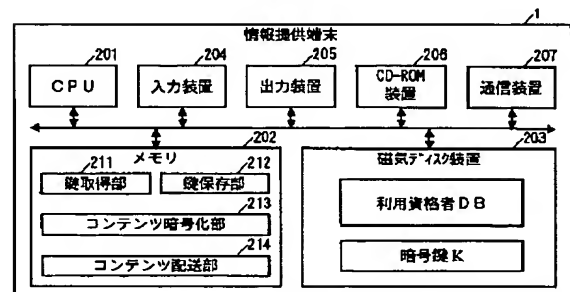
【図 3】

図 3



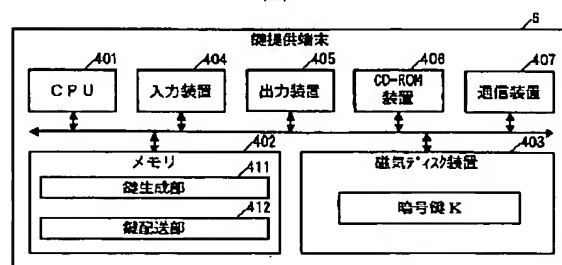
【図 2】

図 2

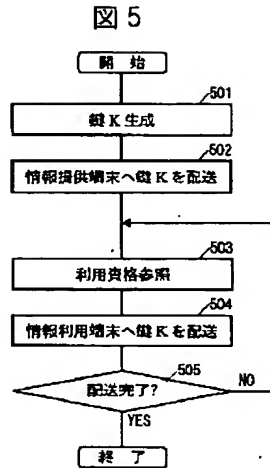


【図 4】

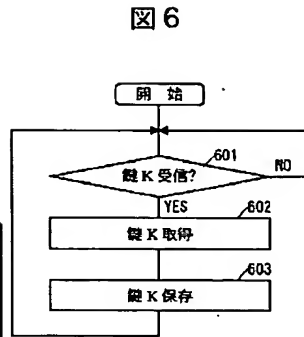
図 4



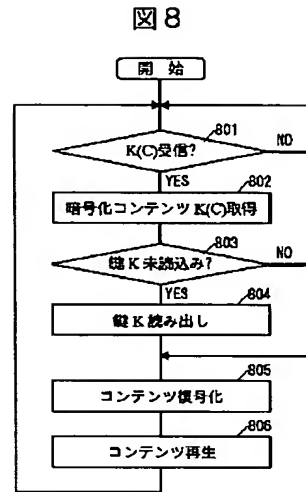
【図5】



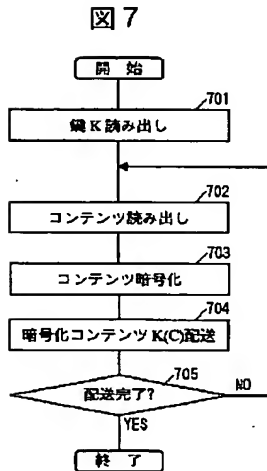
【図6】



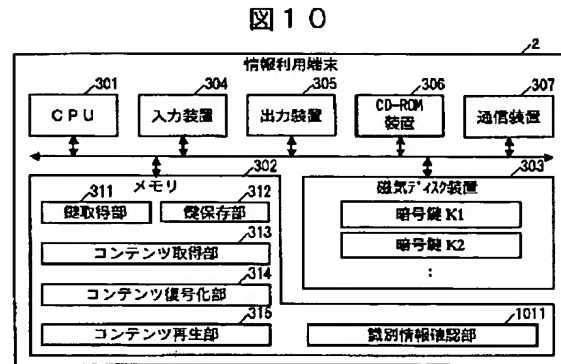
【図8】



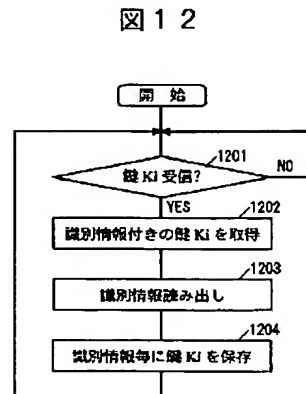
【図7】



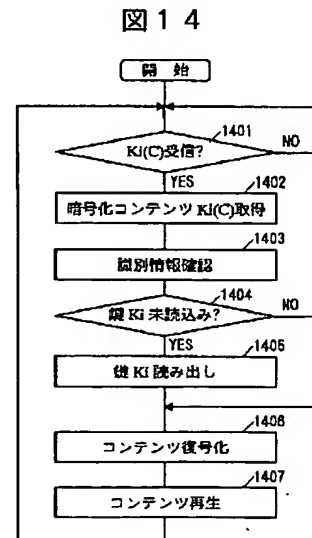
【図10】



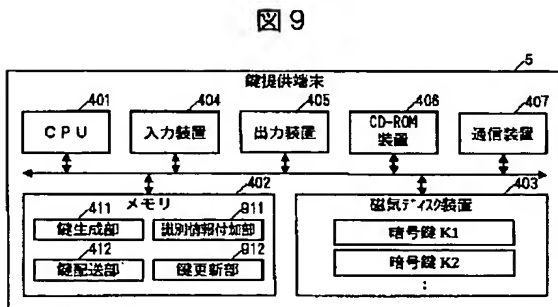
【図12】



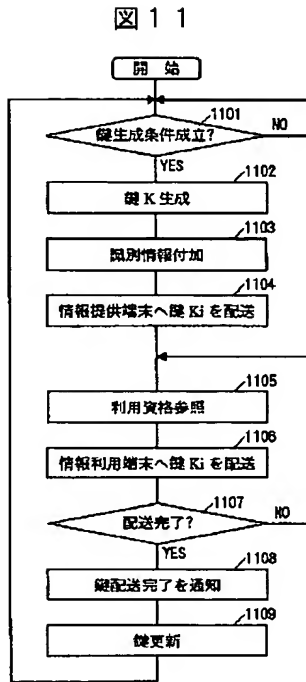
【図14】



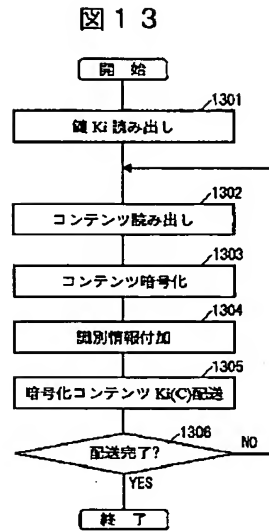
【図9】



【図 11】

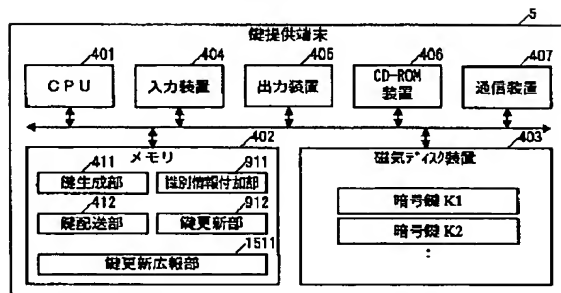


【図 13】



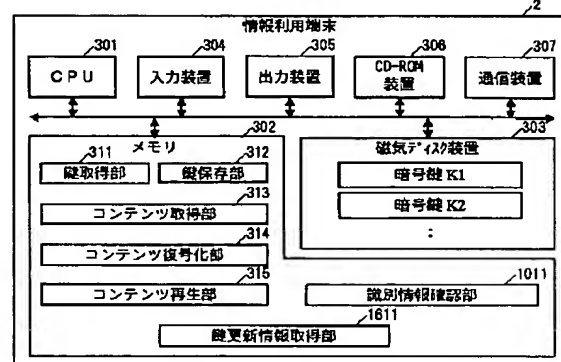
【図 15】

図 15



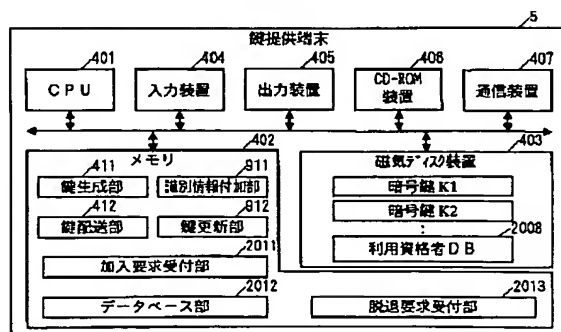
【図 16】

図 16



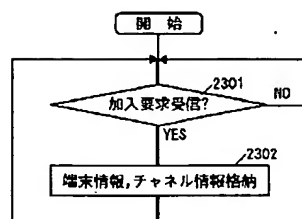
【図 20】

図 20



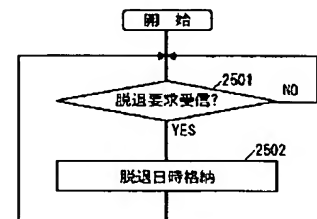
【図 23】

図 23

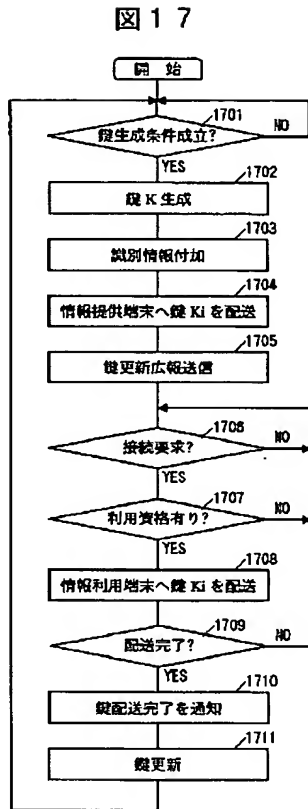


【図 25】

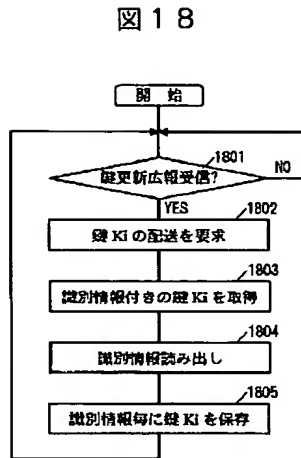
図 25



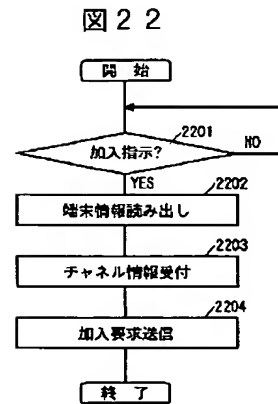
【図 17】



【図 18】

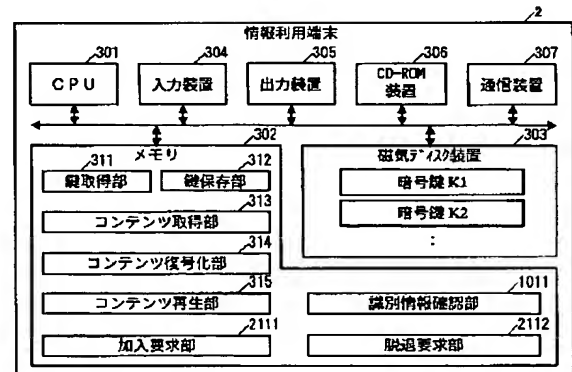


【図 22】



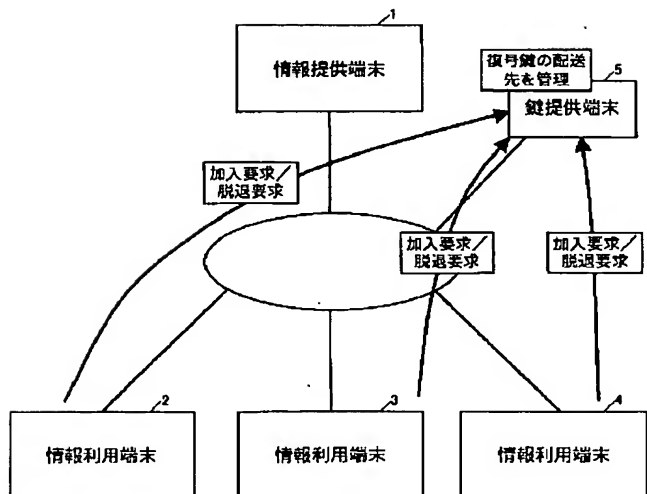
【図 21】

図 21



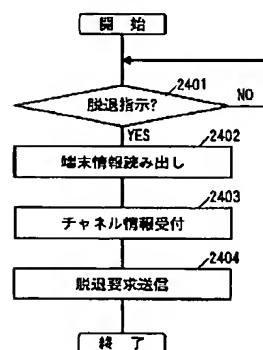
【図 19】

図 19



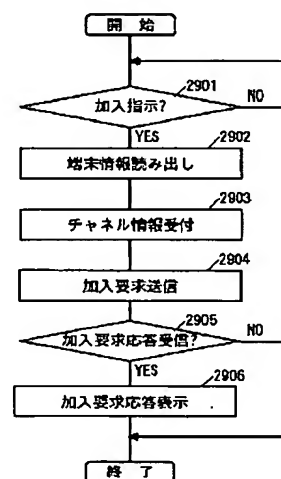
【図 24】

図 24



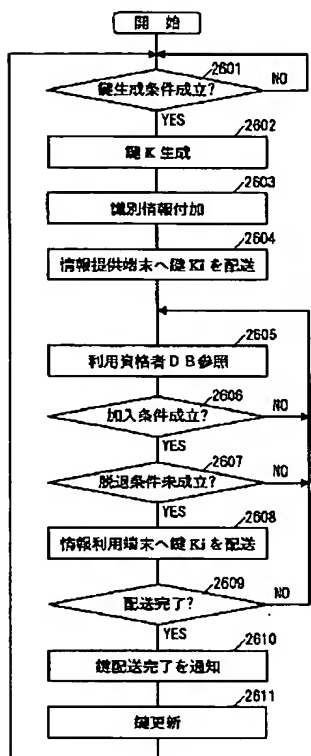
【図 29】

図 29



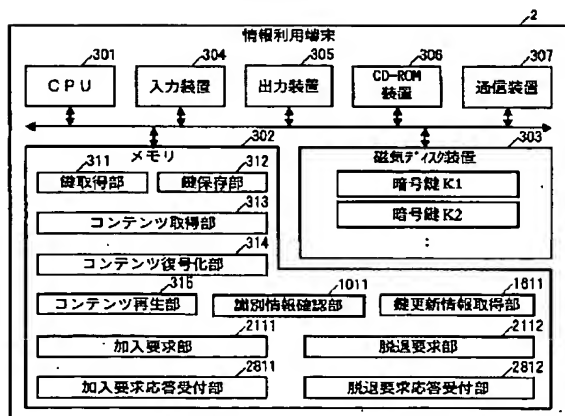
【図 26】

図 26



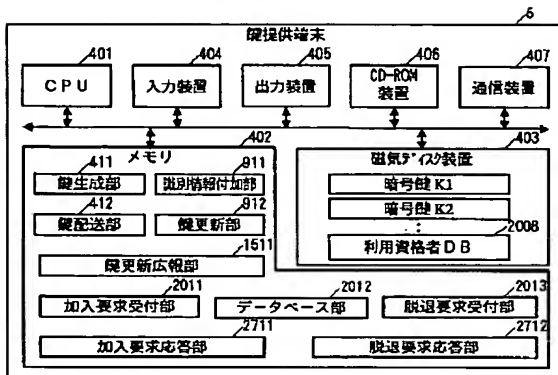
【図 28】

図 28



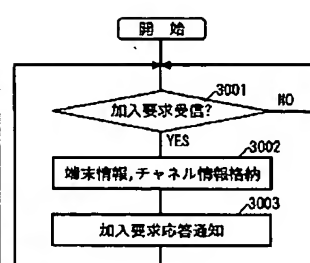
【図 27】

図 27



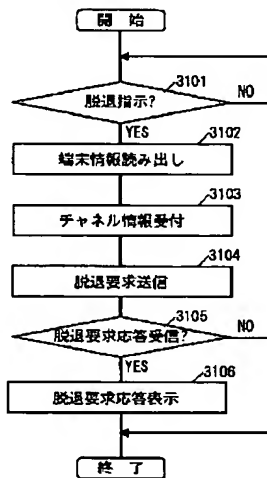
【図 30】

図 30



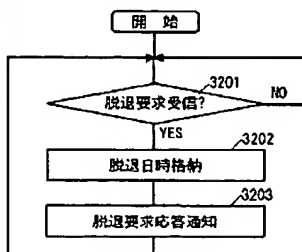
【図 31】

図 31



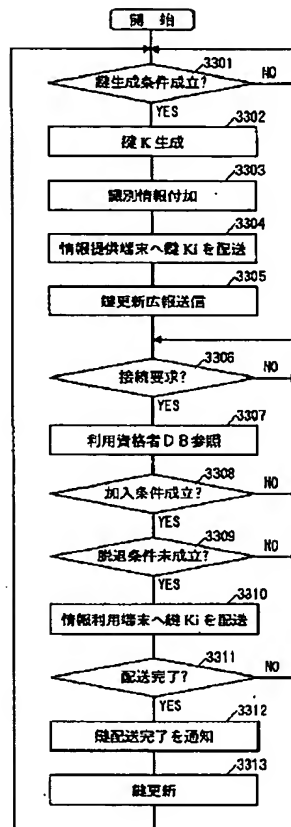
【図 32】

図 32



【図 33】

図 33



フロントページの続き

F ターム(参考) 5B085 AE13 BG07 CA04
 5J104 AA12 AA16 EA04 EA16 EA21
 NA02 PA07
 5K030 GA15 HA08 HC01 LD06 LD19